素数的音乐

The Music of the Primes

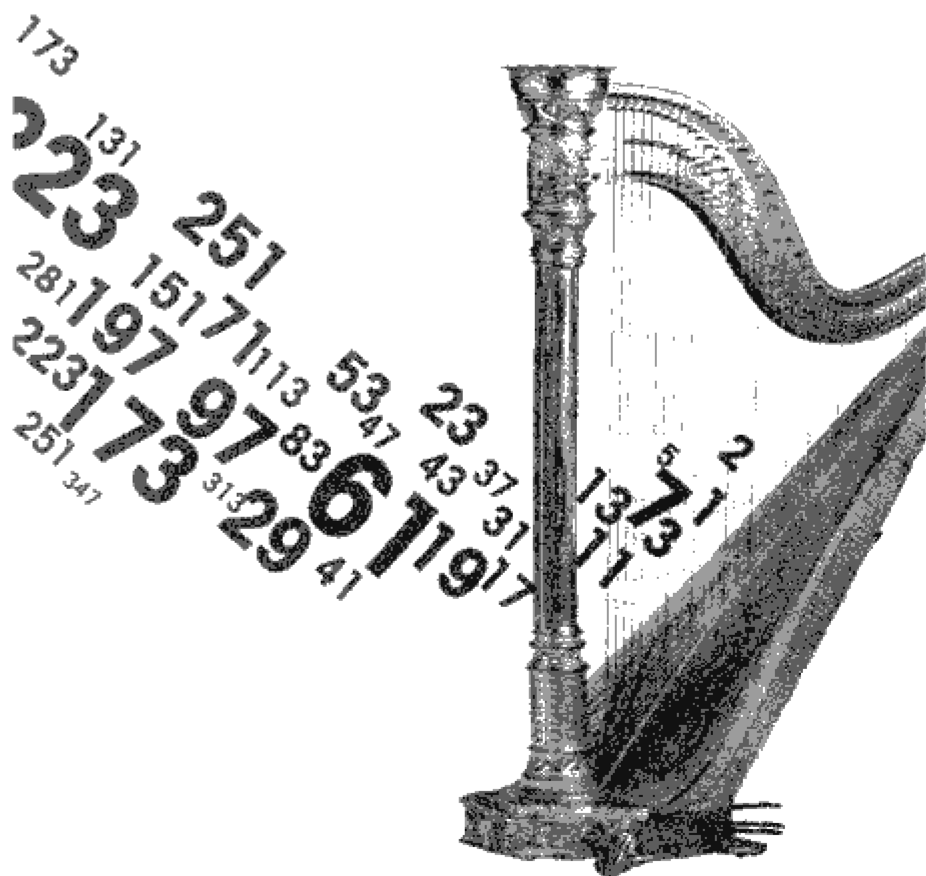


数学圈丛书

素数的音乐

The Music of the Primes

[英]马科斯·杜·索托伊/著　孙维昆/译



湖南科学技术出版社

著作权合同登记号：18－2005－082

本书根据 Harper Collins 2003 年版本译出。

图书在版编目（CIP）数据

素数的音乐/（英）索托伊著；孙维昆译．—长沙：湖南科学技术出版社，2007.4

（数学圈）

书名原文：The Music of the Primes：Why an Unsolved Problem in Mathematics Matters

ISBN 978-7-5357-4873-7

Ⅰ．索．．． Ⅱ．①索．．．②孙．．． Ⅲ．素数-青少年读物 Ⅳ．O156.2-49

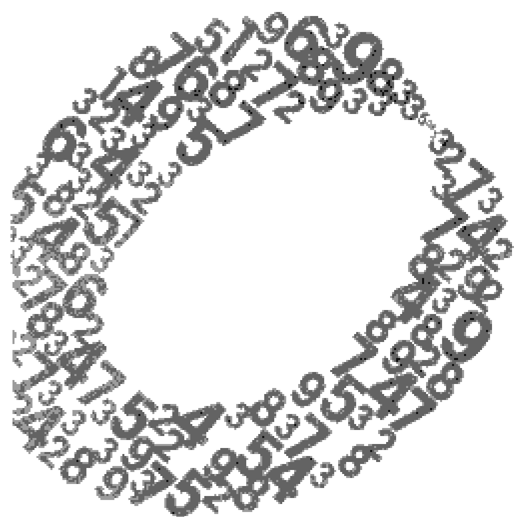
中国版本图书馆 CIP 数据核字（2007）第 051234 号

数学圈丛书

素数的音乐

The Music of the Primes

著　　者：[英] 马科斯·杜·索托伊
译　　者：孙维昆
责任编辑：吴　炜　何　苗
出版发行：湖南科学技术出版社
社　　址：长沙市湘雅路 276 号
http://www.hnstp.com
邮购联系：本社直销科　0731－4375808
印　　刷：长沙瑞和印务有限公司
（印装质量问题请直接与本厂联系）
厂　　址：长沙市井湾路 4 号
邮　　编：410004
出版日期：2007 年 6 月第 1 版第 1 次
开　　本：950mm×670mm　1/16
印　　张：22.75
插　　页：2
字　　数：309000
书　　号：ISBN 978-7-5357-4873-7
定　　价：36.00 元



欢迎你来数学圈

欢迎你来数学圈，那是我们熟悉而陌生的园地。

我们熟悉它，因为几乎每个人都走过多年的数学路，从123走到6月6（或7月7），从课堂走进考场。然后，我们把它留给最后一张考卷，解放的头脑，不再为它留一点儿空间。我们也陌生，模糊的记忆里，是残缺的公式和零乱的图形，是课堂的催眠曲，是考场的蒙汗药……去吧，那些被课本和考卷异化和扭曲了的数学；忘记那一朵朵恶之花，我们会迎来新的百花园。

“数学圈丛书”请大家走进数学圈，也走近数学圈子里的人。这是一套新视角下的数学读物，它不为专门传达任何具体的数学知识和解题技巧，而以“非数学的形式来普及数学”，着重宣扬数学和数学家的思想和精神。它的目的不是教人学数学，而是改变人们对数学和数学家的看法，把数学融入大众文化，回到人们的生活。读这些书不需要智力竞赛的紧张，而是要一点儿文艺欣赏的平和。你可以怀着360样心情来享受数学，经历它的趣味和生命，感悟符号背后的情感和人生。

没有人怀疑数学是文化的一部分，但诺大的“文化”，



却往往将数学排除在外。当然，从人数来看，数学家在文化人中顶多占一个测度为零的空间。但是，数学的每一点进步都影响着整个文明的根基。借一个历史学家的话说，“有谁知道，在微积分和路易十四时期的政治的朝代原则之间，在古典的城邦和欧几里得几何之间，在西方油画的空间透视和以铁路、电话、远距离武器制胜空间之间，在对位音乐和信用经济之间，原有深刻的一致关系呢?”（斯宾格勒《西方的没落·导言》）所以，数学不在象牙塔，就在身边。上帝用混乱的语言摧毁了石头的巴比塔，而人类用同一种语言建造了精神的巴比塔，那就是数学。它是艺术，也是生活;是态度,也是信仰;是最复杂的简单，也是最单纯的完美。

数学是生活。当然，我们的意思不是说生活离不开算术，技术离不开微积分；而是说数学本身也能成为大众的生活态度和生活方式。很多人感觉数学枯燥无味，是因为他把数学从生活中赶走了。当你发现一个小公式也像一首小诗那么多情的时候，还忍心把它忘记吗？大家能享受“诗意的生活”，从这点说，数学是一样的。

数学的生活很简单。如今流行着很多深藏“大道理”的小故事，那些道理多半取决于讲道理的人的态度和立场。它们是多变的，因为多变而被随意扭曲，因为扭曲而成为多样选择的理由。在所谓“后现代”的今天，似乎一切东西都成为多样的，人们像浮萍一样漂荡在多样选择的迷雾里，起码的追求也失落在“和谐”的“中庸”里。数学能告诉我们，多样的背后存在统一，极端才是和谐的源泉和基础。从某种意义说，数学的精神就是追求极端，它永远选择最简的、最美的，当然也是最好的。数学决没有圆滑的道理，也不为模糊的借口留下一点儿空间。

数学生活也浪漫。很多人怕数学抽象，却喜欢抽象的绘画和怪诞的文学。可见抽象不是数学的罪过。艺术家的想象力令人羡慕，而数学家的想象力更多。希尔伯特说过，如果哪个数学家一旦改行做了小说家（真的有），我们不要惊奇——因为那人缺乏足够的想象力做数学家，却足够做一个小说家。懂一点儿数学的伏尔泰也感觉，阿基米德头脑的想象力比荷马的多。我们认为艺术家最有想象力，那是因为我们自己太缺



乏想象力。

数学是明澈的思维。生活里的许多巧合——那些常被有心或无心地异化为玄妙或骗术法宝的巧合，也许只是自然而简单的数学结果。以数学的眼光来看生活，不会有那么多的模糊。有数学精神的人多了，骗子（特别是那些穿戴科学衣冠的骗子）的空间就小了。无限的虚幻能在数学找到最踏实的归宿，它们“如龙涎香和麝香，如安息香和乳香，对精神和感观的激动都一一颂扬。”（波德莱尔《恶之花·感应》）

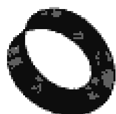
数学是奇异的旅行。数学在某个属于它们自身的永恒而朦胧的地方，在那片朦胧的土地上，我们已经看到了三角形的三个内角和等于180度，三条中线总是交于一点而且三分每一条中线；在那片朦胧的土地上，还存在着无数更令人惊奇的几何图形和数字的奇妙，等着我们去和它们相遇。

数学是纯美的艺术。数学家像画家和诗人，都创造“模式”，不过是用思想来创造，用符号来表达。数学的思想，就像画家的色彩和诗人的文字，以和谐的方式组织起来。数学的世界里没有丑陋的位置。在数学家的眼里，自己笔下的公式和符号就像希腊神话里的那位塞浦路斯国王，从自己的雕像看到了爱人的生命。在数学里，在那比石头还坚硬的逻辑里，真的藏着数学家们的美的追求，藏着他们的性情和生命。

数学是精神的自由。惟独在数学中，人们可以通过完全自由的思想达到自我的满足。不论王摩诘的“雪地芭蕉”还是皮格马利翁（Pygmalion）的加拉提亚（Galatea），都能在数学中找到。数学没有任何外在的约束，约束数学的还是数学。

数学是永不停歇的人生。学数学的感觉就像在爬山，为了寻找新的山峰不停地去攀爬。当我们对寻找新的山峰不再感兴趣，生命也就结束了。

不论你是不是知道一点儿（或很多）数学，都可以走进数学圈，孔夫子说了，“知之者不如好之者，好之者不如乐之者。”只要“君子乐之”，就走进了一种高远的境界。王国维先生讲人生境界，是从“望极天涯”到“蓦然回首”，换一种眼光看，就是从无穷回到眼前，从无限



回归有限。而真正圆满了这个过程的，就是数学。来数学圈走走，我们也许能唤回正在失去的灵魂，找回一个圆满的人生。

1939 年 12 月，怀特海在哈佛大学演讲《数学与善》中说，“因为有无限的主题和内容，数学甚至现代数学，也还是处在婴儿时期的学问。如果文明继续发展，那么在今后两千年，人类思想的新特点就是数学理解占统治地位。”这个想法也许浪漫，但他期许的年代似乎太过久远——他自己曾估计，一个新的思想模式渗透进一个文化的核心，需要 1 000 年——我们的希望是，这个过程会快一点儿，更快一点儿。

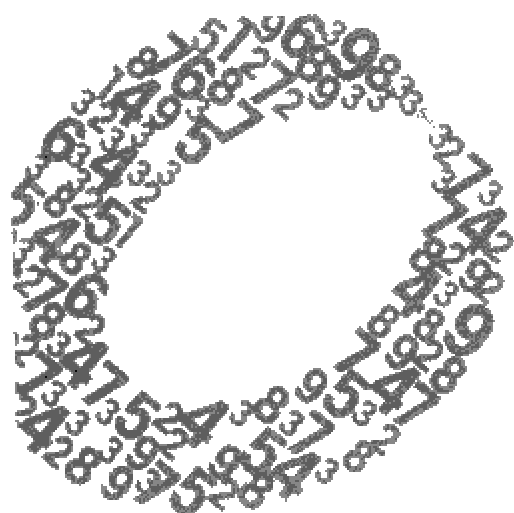
最后，我们借从数学家成为最有想象力的作家的卡洛尔笔下的爱丽思和那只著名的“柴郡猫”的一段充满数学趣味的对话，来总结我们的数学圈旅行：

“你能告诉我，我从这儿该走哪条路吗?”
“那多半儿要看你想去哪儿。”猫说。
“我不在乎去哪儿——”爱丽思说。
“那么你走哪条路都没关系，”猫说。
“——只要能到个地方就行，”爱丽思解释。
“噢，当然，你总能到个地方的，”猫说，“只要你走得够远。”

我们的数学圈没有起点，也没有终点，不论怎么走，只要走得够远，你总能到某个地方的。

李泳

2006 年 8 月



目　录



第一章

谁想成为百万富翁

"关于这列数我们知道什么？好，我们可以来心算……59、61、67……71……这些不都是素数吗？"控制室中弥漫着兴奋的低语。伊莉的脸上短暂地浮现出预感到什么的表情，但是很快的，取而代之的是一种清醒的表情，一种担心被表象干扰而导致愚蠢的、不科学的理解的表情。

——卡尔·萨根（Carl Sagan），《接触》（*Contact*）

1900年8月的一个闷热的上午，巴黎大学拥挤的报告厅中，来自哥廷根大学的大卫·希尔伯特为国际数学家大会作报告。已经是当时最伟大的数学家之一的希尔伯特准备了一场大胆的演讲，他打算讨论的是那些未知的问题，而不是已经证明的结果。由于这不符合传统，当希尔伯特开始展示自己对数学未来的看法时，听众们甚至可以听出他嗓音中的紧张。"在我们之中谁不乐意拉开这块隐藏着未来的大幕，并对未来世纪中科学的下一个进展及其发展的秘密投上关注的一瞥呢？"预示着新世纪的到来，希尔伯特用23个问题对听众提出挑战，他相信这23个问题将为20世纪的数学探索者们设定好方向。

有不少希尔伯特问题在随之而来的世纪中得到了解决，而解决这些问题的杰出数学家就是所谓的"荣誉一族"，其中包括了哥德尔、庞加莱、以及许多用思想改变数学世界的先锋们。但是仍然有一个问题——希尔伯特第八问题，经过了整个世纪仍然无人能攻克，这就是黎曼

假设。

在希尔伯特设下的挑战中，第八问题在他心中有着特殊的地位。有一个关于巴巴罗萨的德国传说，这位受人爱戴的德国国王逝世于第三次十字军东征时期，但是在民间传说中他并没有死去，而是沉睡在基夫霍伊瑟山脉（Kyffhäuser Mountains）的某个山洞中，当德国需要他的时候他就会醒来。因此有人问希尔伯特："如果你可以像巴巴罗萨那样在500年后醒来，你会做什么？"希尔伯特回答说："我会问，'有人证明黎曼假设了吗？'"[1]

在20世纪接近尾声的时候，大部分数学家都接受了这个事实：这颗希尔伯特问题中的宝石不光在本世纪无法解决，也许在希尔伯特沉睡500年后醒来时仍然无法解决。在20世纪第一场国际数学家大会上，希尔伯特那充满未知的革命性的演讲深深地触动了数学界；然而，当大家在筹备20世纪最后一场国际数学家大会的时候，有一个惊喜即将出现。

1997年4月7日，一条特殊的新闻闪现在国际数学界的网络中。在即将于次年举办的德国柏林国际数学家大会的网页上，有人宣称证明了数学中的圣杯——黎曼假设。由于黎曼假设问题是数学的核心问题，如果这条新闻是真的，它将产生极其深远的影响。因此所有收到电子邮件的数学家都紧张地期待着能了解这个最重要问题的证明。

这封邮件源自恩里克·邦比艾里（Enrico Bombieri）教授，从信息的来源方面讲，再没有比邦比艾里教授更好的人选。邦比艾里教授是黎曼假设的守护者之一，他目前就职于声望极高的普林斯顿高等研究院，这里也曾经是爱因斯坦和哥德尔工作过的地方。尽管他在电子邮件中说得很婉转，但是数学家仍然不敢掉以轻心。

邦比艾里在意大利长大，受家族繁荣的葡萄园生意的影响，他的品位不凡，喜欢追求奢华的生活，因此同事们都亲切地称他为"数学贵族"。年轻时，他总是开着炫目的跑车参加欧洲学术会议，出尽了风头。有一则传言说他曾六次参加意大利24小时拉力赛，对此他并没有反驳，而是十分高兴地默认这一点。20世纪70年代，由于在数学上的成功，



邦比艾里获得了普林斯顿的邀请。到普林斯顿后，他仍然不改当年本色，只是热情从拉力赛转到了绘画（尤其是肖像画）。

然而邦比艾里最大的爱好却是创造性的数学，尤其是黎曼假设的挑战。早熟的他在15岁首次读到黎曼假设的时候，就已经深深地被它迷住了。他在翻阅身为经济学家的父亲的数学书籍时，就深深地被自然数的美妙性质迷倒，并将其收集到自己的知识宝库中。邦比艾里知道黎曼假设是数论中最深刻也是最基本的问题，为此他的父亲允诺他，如果他能解决黎曼假设就买一部法拉利给他，从此他对黎曼假设的热情一发不可收拾，虽然这是他父亲试图阻止他一意孤行的绝望尝试。

2

根据邦比艾里的电子邮件，他再也无缘得到法拉利。信的开头如下，“阿兰·科纳（Alain Connes）在上周三于高等研究院所做的报告中提到了一些有趣的进展”。数年之前，阿兰·科纳转向研究黎曼假设的新闻曾震惊了数学界。科纳是该领域的革命家之一，如果说邦比艾里是路易十六，那么科纳就是温和派的罗伯斯比尔[①]。他具有一种超凡的气质，他的热情与其他数学家平静、沉稳的形象相去甚远。他有一种使别人信服其观点的能力，他的讲座令人着迷。他的追随者们视他为领袖，他们乐于追随他并为其挺身而出，来保护他们的英雄免受保守派的进攻。

科纳就职于巴黎的高等科学研究院（IHES，Institut des Hautes Études Scientifiques），这相当于法国的普林斯顿高等研究院。自从1979年到此以来，科纳已经创造了一种全新的语言来理解几何。科纳从不害怕将数学带到极端抽象的境地，甚至大部分习惯在家中利用高度抽象的数学概念来理解世界的数学家，都不愿面对科纳提出的抽象革命。然而正如他向那些怀疑他的古板理论是否必要的人展示的那样，他的几何学新语言包含着许多真实量子物理世界中的线索。如果这样做会给数学主体部分带来恐惧，那也无所谓。

3

---

① Maximilien Robespierre，1758～1794，法国革命家，是法国大革命时期重要的领袖人物，是雅各宾派政府的实际首脑之一。（本文中的脚注如不加说明，均为译者所加。）



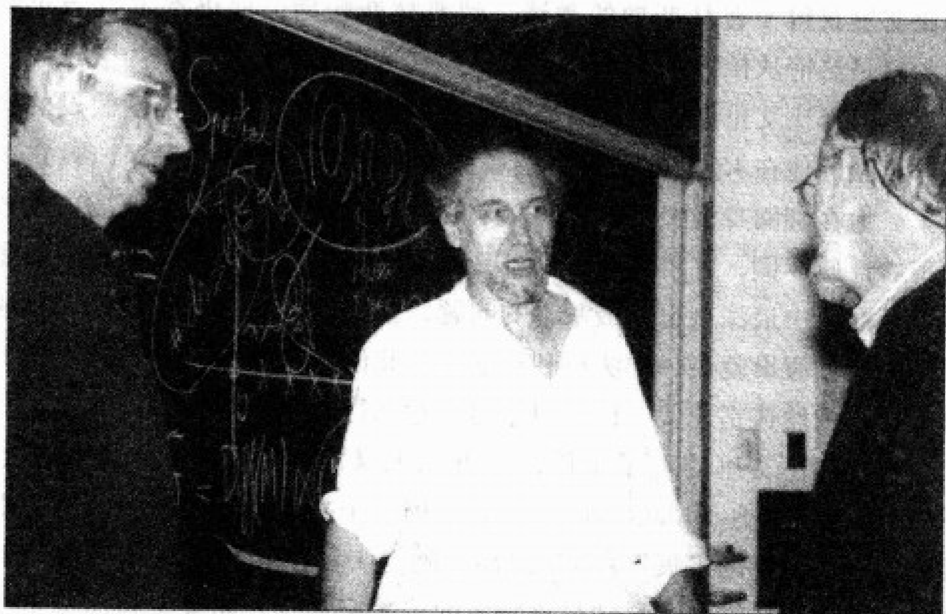
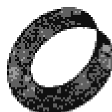


图1　阿兰·科纳，IHES及法兰西学院教授

科纳相信，他的新几何不仅可以揭开量子物理世界的面纱，而且可以解释黎曼假设——有关于数的最神秘定理。人们对其大胆的信念纷纷表示惊奇和震惊，这反映了他根本不受传统的约束，敢于闯人数论的核心并与数学中最困难的难题正面交锋。自从他于20世纪90年代中期参与这项工作之后，大家都认为，如果还有人能解决如此著名的难题，那一定是阿兰·科纳。

但看起来并非科纳找到了复杂拼图的最后一片，邦比艾里接着解释道，而是听众中的一位年轻物理学家灵光一闪，突然明白了如何运用他的“超对称费米-波色系统”来解决黎曼假设。许多数学家并不明白这个混合众多专业术语的名词的真正含义，但是邦比艾里解释道，它描述了“由具有相反自旋的anyon粒子和moron粒子①混合而形成的接近绝

① 这是邦比艾里自造的两个新词，表示两种新粒子，在实际中并不存在，详见后文。



对零度的热力学系综这样的物理现象"。虽然这一番话听上去仍是模糊不清，但这毕竟是数学中最难问题的解答，大家也不期望有一个简单的解决方案。据邦比艾里的邮件，经过六天不间断的工作，以及一种新的计算机语言 MISPAR 的帮助，这位年轻的物理学家最终解决了这个数学难题。

邦比艾里的邮件如此结束，"哇！请尽可能广泛地转发此消息。"尽管一位年轻的物理学家证明了黎曼假设，有点儿异乎寻常，但并未引起太大的惊奇，因为数十年来大部分数学家均发现该问题与物理学联系紧密。作为一个数论核心问题，黎曼假设近年来越来越多地与粒子物理中的问题产生了意料之外的共鸣。

数学家纷纷改变行程飞到普林斯顿，希望能分享这一刻。人们也许还记得数年之前，同样的激动场面发生在另一位英国数学家安德鲁·怀尔斯（Andrew Wiles）宣称给出费马大定理①证明的时候。1993 年 6 月，怀尔斯在剑桥作报告时宣称费马大定理是正确的，即 $x^n + y^n = z^n$ 在 $n > 2$ 时无解。当怀尔斯放下粉笔的那一刻，报告厅中立刻充满了香槟和闪光灯。

4

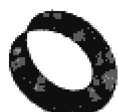
数学家们都明白，对于数学的未来而言，证明黎曼假设有着比知道费马方程无解远远大得多的影响。如同邦比艾里 15 岁就知道的那样，黎曼假设本质上是试图理解数学中最基本的元素——素数。

素数是算术的原子，是那些不能写成两个较小的数之乘积的数。13 和 17 就是素数，而 15 不是，因为 15 等于 3 乘以 5。素数就是镶嵌在数之宇宙上的宝石，而这个宇宙已经被数学家研究了数个世纪。对于数学家而言，2，3，5，7，11，13，17，19，23，…这些无穷无尽的数存在于一个与我们的现实世界完全独立的空间中，它们是大自然给数学的恩赐。

素数对于数学的重要性在于，它们的乘积可以生成其他的数。每个非素数的数（称为合数）都可以写成素数的乘积。物理世界中的每一个

---

① 也称为费马最后定理（Fermat Last Theorem）。



分子都是由元素周期表中的原子构成，素数表就是数学中的元素周期表。在数学实验室中，素数2，3，5就相当于氢、氦、锂。掌握了这些基本元素之后，数学家就有希望找到新方法，来标注复杂数学世界中的前进道路。

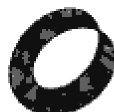
抛开本身的简单性和基本性，素数仍然是许多数学家研究的最神秘对象。其中一个分支是研究素数的分布规律，这对于数学家而言是一个根本挑战。如果你观察素数分布表，就会发现想要预测下一个素数何时出现几乎是不可能的。素数表的无序、随机，使得人们无法找出决定下一个素数的线索。素数表反映了数学的心跳，只是这个心跳的节奏被加了咖啡因的鸡尾酒所打乱。



图2　小于100的素数，数学的不规则心跳

是否能找到一个生成素数的公式？或是某个奇妙规则能告诉你第100个素数是什么？自古以来这些问题就折磨着数学家。经过2000多年的努力，要找出一个直观的素数分布仍然是无望的。数个世纪以来，人们一直倾听着素数自身的心跳，两下、三下、然后是五下、七下和十一下，如此继续下去，于是人们开始相信这些随机的心跳是没有任何内在逻辑的随机的噪音。尽管数学的核心是追求有序性，但是在素数表中，数学家唯一能观察到的只是无序。

大自然如何选择素数，也许根本没有一个合理的解释，但是数学家无法坦然接受这一结果。如果失去了结构，没有了优美的简单性，那数学也就不值得研究了。听着这样无序的噪音从来就不是一件愉快的事情，正如法国数学家亨利·庞加莱（Henri Poincaré）所写的，“科学家从不会为了有用而研究大自然；科学家研究大自然只因为能在过程中获得乐趣，而乐趣正来自于大自然的优美；如果大自然不是优美的，那它根本不值得被了解；如果大自然不值得被了解，生命也不再有任何



意义。"

也许有人觉得素数的不规则性只出现在最初，慢慢地就会稳定下来。但事实并非如此，情况只会随着数的增大而更糟。在此我们给出10 000 000上下100个数中的素数，首先是小于10 000 000的素数：

9 999 901　9 999 907　9 999 929　9 999 931

9 999 937　9 999 943　9 999 971　9 999 973

9 999 991

然后让我们看看大于10 000 000的素数有多少：

10 000 019　10 000 079

对于这种情况，猜出其中蕴涵的公式几乎是不可能的。与其说素数序列有序，倒不如说它是随机的更恰当。就如同已知前99次掷出的硬币朝向，你还是不能预测第100次究竟是哪面朝上。素数也是同样的不可预知。

素数问题给数学家带来了该学科中最不寻常的紧张状态。一方面，一个数不是素数就是合数，你将硬币翻过来也不可能让某个素数被更小的数整除；同时不可否认，素数表看上去就是随机选取的数列。物理学家逐渐接受一个观点，即量子骰决定了宇宙的命运，量子骰的每次抛出都随机决定哪里存在物质。但是如果承认大自然是通过掷骰子来决定数学中这些最基本的数的命运，将是一件非常尴尬的事。数学家不可能接受随机和无序。

6

抛开其随机性，素数的永恒性和普适性更胜于数学的其他概念。无论我们对它们的认识进步到何种程度，它们始终都在那里。剑桥的数学家哈代（G. H. Hardy）在其著名的《一个数学家的自白》中说道，"317是个素数，并非因为我们这样认为，也非因为我们的思维是以这样或那样的方式形成，而是因为它原本如此，因为数学实在（mathematical reality）就是这样建立的①。"

① 凡本文中涉及哈代在《一个数学家的自白》中的引文均引自江苏人民出版社1999年版《科学家的辩白》（哈代、维纳、怀特海著，毛虹等译）。



某些哲学家对于世界也抱有同样的柏拉图主义观点——这是对超越人类存在的、绝对和永恒的实在的信念——但是对我而言，这正是他们为什么是哲学家而不是数学家的原因。这里有一段阿兰·科纳（就是邦比艾里邮件中出现的那个人）和神经生物学家让-皮埃尔·项杰（Jean-Pierre Changeux）在《关于思想、物质和数学的对话》中的富有感染力的对话，这本书显露出紧张的气氛，即数学家认为数学的存在性是超越思想的，而神经学家则试图反驳："为什么我们不能在天空中看见金色的'$\pi=3.1416$'字样，或是在水晶球的反光中看见'6.02×10^{23}'？"科纳坚持"确实存在着独立于人类思想的、原始的、永恒的数学实在"，并且在那个世界中，我们可以找到永恒不变的素数表。项杰对此表达了自己的失望之情。但科纳坚持认为数学"毫无疑问是仅有的普适语言"。在另一个世界中完全可以存在一种不同的化学或生物学，但是无论你在哪个星系中计数，素数都还是素数。

在卡尔·萨根的著名小说《接触》中，外星人利用素数来联系地球上的生命。书中的女主人公伊莉·阿若薇（Ellie Arroway）在SETI（Search for Extraterrestrial Intelligence，地外文明搜索）工作，倾听来自宇宙中的电波。某天晚上，当射电望远镜指向织女星的时候，他们从背景辐射中收到了奇怪的脉冲。伊莉花了一些时间分析电波讯号中的规律，2次脉冲后停一下，紧接着是3次、5次、7次、11次，就这样沿着素数一直到907，然后重新循环。

这个宇宙的鼓点演奏出一首地球人熟悉的音乐。伊莉意识到只有智慧生命才能送出这样的讯号，"难以想象这些射电脉冲居然传送了如此有规律的数学讯号，正是这些素数吸引了我们的注意力。"如果这些外星人没有持续十年不断地发送这些幸运的讯号，伊莉肯定不能从背景辐射中辨认出它。尽管这些素数如同彩票中奖号码那样随机，但是它们普适的不变性决定了外星广播如何选择每个数字，正因如此伊莉认识到这种排列是智慧生命的标志。

7

利用素数来传递信息不光出现在科幻小说中。奥利弗·萨克斯



(Oliver Sacks) 在《错把太太当帽子的人》① 中记录了这样一件事，一对26岁的双胞胎，约翰和麦克尔，他们通过交换六位素数进行交流。萨克斯首次发现他们在屋角秘密交换着数字时，“他们乍看上去像两个品酒的专家，正在分享着少见的口味。”起初萨克斯并不知道他们在干什么，直到他破解了他们的密码之后。他默默地记了一些八位的素数并在他们下一次交流的时候，偷偷地加入进来。双胞胎先是吃了一惊，然后就陷入沉思，最后他们欢呼起来，因为他们找到了下一个素数。萨克斯求助于素数表来找出素数的时候，双胞胎是如何找到素数的，这显然还是个谜。是不是这些孤僻的天才掌握了某些秘密公式，而这些公式却是数学家错失的？

邦比艾里特别喜欢这个双胞胎的故事：

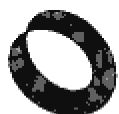
> 听到这个故事，我无法掩饰自己对大脑功能的敬畏和惊奇。但是我想问，我的那些非数学家朋友是否也有同样的能力；或者他们曾有过一些如这对双胞胎所拥有的那些奇异的、惊人的和超凡的奇妙天赋。他们是否知道，数学家奋斗了几百年，就是为了做约翰和麦克尔在一起做的事情：生成和识别素数。

在有人能找出他们是如何做到这一切的原因之前，这对双胞胎在37岁时被他们的医生分开，因为医生认为他们独有的数字语言阻碍了他们的发展。如果这些医生听过大学数学系公共休息室里的神秘语言之后，说不定也会推荐将这些数学家关禁闭。

现在看来，这对双胞胎可能是使用一个基于费马小定理的技巧来判断一个数是否为素数。双胞胎在电视脱口秀节目中表演的技巧和自闭症天才能迅速判断出1922年4月13日是星期四的方法类似，这些技巧都使用了一种叫做时钟算术或模算术的方法。即使他们没有素数公式，他

8

① *The Man Who Mistook His Wife for a Hat* 是神经医学专家奥利弗·萨克斯的通俗文学著作，其中记载了他碰到的临床案例。



们的技巧仍然是超乎常人的。在他们被分开之前，他们已经可以识别和生成二十位的素数，这远远超过萨克斯的素数表的上限。

正如萨根的女主角倾听宇宙的素数心跳，和萨克斯偷听双胞胎的素数一样，数学家数个世纪以来为找出这个噪音中的规律而竭尽全力。但是像西方人听东方的音乐一样，所有的音符都毫无意义。不过，到了19世纪中期，关键的突破终于出现。伯纳德·黎曼（Bernhard Riemann）用一种全新的方式来审视这个问题，从这种新观点来看，在素数表面的噪音之下潜藏着微妙的、意料之外的和谐。尽管这是不小的进步，但这首全新的乐曲仍然有许多秘密超越我们的听力。数学世界的瓦格纳，勇敢的黎曼做出一个关于这首神秘乐曲的大胆预言，这个预言就是我们所知的黎曼假设。它是黎曼关于这首乐曲的直觉体现，只要有人能证明黎曼假设的正确性，就能解释为何素数表现出如此强烈的随机性。

黎曼的洞察力来自于他发现了一面数学魔镜，通过这面魔镜他可以凝视素数。当艾丽思穿过魔镜时，整个世界发生了翻天覆地的变化。同样，在黎曼魔镜背后的神秘数学世界中，素数的无序转变成数学家渴望多年的有序。黎曼猜想无论魔镜后面的世界多么广阔，这个规律将永远不会改变。黎曼关于魔镜背后的世界所蕴涵的内部和谐的预言可以解释素数的外在无序性。绝大部分数学家都认为，由黎曼魔镜带来的，将无序变为有序的改变，简直就是不可思议的结果。因此，黎曼留给后人的挑战，就是证明黎曼所洞悉的规律确确实实存在于那里。

邦比艾里于1997年4月7日发出的邮件，宣告了一个新时代的开始。黎曼的想象并非是幻想，“数学贵族”已经为数学家展现了这种解释存在的可能性，这将说明素数的表面无序性。由于这个伟大问题的解决，数学家也迫不及待地由此挖掘出更多的未知事物。

9

黎曼假设的结论将对其他许多数学问题带来巨大影响。由于素数对于数学家而言是如此的基本，因此任何关于素数本质的发现都会产生大规模的影响，黎曼假设就是这样的一个问题。当数学家在数学世界中寻找前进的方向时，似乎所有的道路都不可避免地路过这个著名的景点



——黎曼假设。

许多人将解决黎曼假设与登上珠穆朗玛峰相比较。离顶峰越远，我们征服它的欲望越强；最终登上黎曼高峰的数学家毫无疑问会比埃德蒙·希拉里[1]更加不朽。征服珠峰的奇妙之处并不是因为峰顶是一块特别令人兴奋的土地，而是因为整个攀登过程中遇到的挑战。从这方面讲，解决黎曼假设显然不同于登上世界最高峰。如果我们能够登上“黎曼峰”，那么“黎曼峰”就是我们渴望坐下来的那块土地，因为我们早已知道将要面对的景色。许多数学家为了证明自己的结论而假设黎曼假设为真，因此最终证明黎曼假设的人将为这数千个定理的证明补上漏洞。

正因为有如此多的结论依赖于黎曼提出的挑战，所以我们宁愿称它为“假设”而不是“猜想”[2]。因为“假设”一词所蕴涵的强烈意义，就是数学家试图在此基础之上建立一套理论；相比较而言，“猜想”一词仅仅表示数学家对这个世界的行为方式的预言。许多人在无力推翻黎曼假设的情况之下，不得不将该假设当作是成立的事实。如果真有人可以将这个假设变为定理，那么其他所有未证明的结论将会随之成立。

由于对黎曼假设的依赖，数学家不得不赌上了自己的名誉，期望有一天某人能证明黎曼的直觉是正确的。更有甚者，认为承认它是一个有效的假设还不够。邦比艾里认为这是不容怀疑的信条，素数的行为与黎曼假设预言的一致。因此，黎曼假设实际上成为了追寻数学真理的基石。但是话说回来，如果黎曼假设被证明是错误的，这将彻底摧毁我们持有的信念，即我们的直觉能感知万事万物如何运转。正因为我们如此坚信黎曼假设的正确性，当另一种结论出现时，我们有关数学世界的观点就要发生根本的改变。当然我们曾相信的、所有依赖于黎曼假设的结

---

① Edmund Hillary，新西兰人，1953 年与尼泊尔向导丹增诺吉成为首次登上珠穆朗玛峰的人，后被英国女王授予爵士称号。

② 在数学中，一般未经证明的命题被称为猜想（Conjecture）。而黎曼假设的英文是 Riemann Hypothesis。



论也将灰飞烟灭。

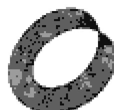
最值得注意的是，黎曼假设的证明即意味着数学家可以利用一个非常迅速的程序来定位一个一百位或任意位数的素数。你也许会问："那又怎样?"当然除非你是一个数学家，否则这样的结果看上去不太可能对你的生活产生巨大影响。

找出一个一百位的素数，看上去如同数针尖上的天使一样无意义①。虽然许多人知道数学存在于一架飞机和电子技术的背后，但很少有人承认这些深奥的素数世界会给他们的生活带来影响。早在19世纪40年代，哈代就有着同样的想法，"这样高斯和另一些数学家就应该庆幸至少还有一种科学（数论），由于其远离人类日常的活动而保留了其纯洁性。"

不过随着最近的一系列事件，素数走上了粗俗、肮脏的商业世界的中心舞台，而不是仅仅局限在数学的城堡中。在20世纪70年代，三位科学家罗恩·瑞威斯特（Ron Rivest）、阿迪·沙米尔（Adi Shamir）和莱昂纳德·阿德曼（Leonard Adleman）使得追寻素数这件事，不再是学术界象牙塔中偶尔的游戏，而是变成了重要的商业应用。从皮埃尔·德·费马（Rierre de Fermat）在17世纪的一个发现出发，三位科学家找到了一种利用素数来保证我们的信用卡在电子商务或全球市场中安全使用的方法。当这个思想于20世纪70年代刚被提出时，没有人能预料电子商务的未来会有多么广泛；但是到了今天，缺少了素数的保护，电子商务将寸步难行。每次你在网站上下订单时，你的计算机都依赖于一个一百位的素数提供的安全。这个密码系统以三位发明者姓氏的首字母来命名，即RSA密码系统。迄今为止，有超过一百万个素数被用来保护电子商务的安全。

因此，每个基于因特网的商业贸易都依赖于一百位的素数来保证商

① "针尖上能站几个天使?"是欧洲中世纪教会经院哲学问题之一，传说牛顿晚年曾研究过这个问题。



业传输的安全，而因特网不断扩大的重要性将导致我们每个人都需要自己的独立素数，以便于被唯一地识别。因此突然间，商业界也对黎曼假设的证明究竟是否能够对素数在数的宇宙中如何分布产生帮助，发生了兴趣。

这件事的特别之处在于，尽管这个密码的“生成”依赖于费马在300多年前发现的关于素数的结果，但是如何“破解”这个密码仍然是我们无法回答的问题。RSA密码系统的安全性就是建立在我们无法解决最基本的素数问题的基础之上。数学家对于生成因特网密码的素数了解的足够多，但是却无法破解它。我们能理解方程的一半，可我们却不能了解另一半。然而，如果我们揭开素数神秘外衣越多，因特网上密码的安全性就越低。这些素数就是钥匙，用它能够打开全世界电子秘密的锁。这也就是为什么像AT&T① 和惠普这样的公司愿意投资金钱，试图了解素数背后的微妙之处以及解决黎曼假设。这些努力也许能破解这些素数密码，而何时这些密码开始失效，也是所有涉及因特网的公司都想最先知道的。这也正是为什么数论和商业会奇怪联姻的原因。商业机构和安全部门正紧盯着纯数学的黑板。

因此对邦比艾里的声明感兴趣的并不仅仅是数学家。黎曼假设的解决是否会导致电子商务的崩溃？美国国家安全局（National Security Agency）的特工们也被派到普林斯顿，寻求这个问题的答案。在数学家和特工们纷纷聚集到新泽西的时候，一些人领悟到了邦比艾里邮件中的微妙之处。基本粒子一般用古怪的名称来命名：胶子（gluons），级联超子（cascade hyperons），粲介子（charmed mesons），夸克（quarks），其中最后一个来自詹姆斯·乔伊斯（James Joyce）的著作《芬尼根守灵夜》（Finnegans Wake）。但是morons？显然不符合这一原则!②。邦比艾

---

① 美国电报电话公司，全名为American Telephone & Telegraph Company，由电话发明人贝尔于1877年创建，曾长期垄断美国长途和本地电话市场。AT&T在近20年内，经过多次分拆和重组，目前仍是美国最大的本地和长途电话公司。

② moron在英文中有傻子、低能者的意思。



里作为该领域的权威，他能正确评价那些有关黎曼假设的尝试，但是清楚他个人性格的人也知道，他其实具有一种淘气的幽默感。

当人们发现安德鲁·怀尔斯在剑桥提交的费马大定理的证明中存在一个漏洞的时候，曾怀疑这是一个愚人节的玩笑。不过这一次，邦比艾里的邮件开了整个数学界一个玩笑。由于太渴望再次经历像证明费马大定理那样的兴奋，数学家中了邦比艾里的计。由于大家的兴奋，以至于原本信件中存在的 4 月 1 号的字样也在转发中消失不见。由于这个原因，再加上有些国家没有愚人节这个概念，因此这个玩笑的结果远超邦比艾里原先的想象，最终邦比艾里不得不出面承认这是个玩笑。因此，在 21 世纪到来之际，我们对数学中最基本的数的认识仍然是处于一片黑暗之中，是素数笑到了最后。

12

为什么数学家会相信邦比艾里而受骗？并非是他们轻易地放弃了这个荣耀。在宣布一个结果被证明之前，数学家所经历的严格检验远远超过那些其他学科中看上去已经足够的检验。当怀尔斯证明费马大定理的初稿被人发现漏洞时，他意识到拼图游戏即使完成了 99% 也是不够的：完成最后那 1% 的人才真正会被人们记住，而这样的 1% 往往多年也得不到解决。

搜寻素数的秘密之源已经持续了 2000 多年，对这个万能药的渴望导致数学家轻信了邦比艾里的玩笑。多年来，不少数学家仅仅因为害怕而不敢接近这个著名难题的领域。但令人惊讶的是，在接近世纪末的时候，有越来越多的人打算攻克这个难题。也许是费马大定理的证明，点燃了大家的希望，原来难题也是可以被证明的。

13

怀尔斯解决了费马大定理，从而引起世人对数学家的关注，这是数学家希望得到的关注，无疑也正是这种心情促使大家相信邦比艾里。出人意料的是，怀尔斯还曾被邀请为 Gap 男装长裤做模特，这个感觉很好，原来数学家也可以如此性感。数学家在自己的世界中倾注了太多的时间，虽然这可以给自己带来兴奋和快乐，但这种快乐很难与世人一起分享。现在他们终于得到一个机会，可以向世人炫耀自己的战利品，那





图 3　恩里克·邦比艾里，普林斯顿高等研究院教授

些他们经过长途跋涉而发现的财宝。

证明黎曼假设将标志着 20 世纪数学的光辉顶点。希尔伯特留给数学家的挑战，揭开了这个世纪的序幕，也是全球数学家渴望破解的谜。而在希尔伯特提出的 23 个问题中，黎曼假设是唯一一个未被征服而进入 21 世纪的问题。

2000 年 5 月 24 日，为了纪念希尔伯特问题提出 100 周年，数学家和媒体再次聚集到巴黎的法兰西学院（Collège de France），等待一组全新 7 个问题的发布，这是为了迎接新千年的到来而向数学界提出的挑战。包括了安德鲁·怀尔斯和阿兰·科纳在内的世界顶尖数学家组成的



小组挑选了这7个问题。7个问题中的6个都是全新的，除了在希尔伯特的名单中出现过的那个问题——黎曼假设。出于对改变了20世纪的资本主义思想的尊重，这些挑战都带有赏金。黎曼假设与其他6个问题的价码，分别都是100万美元。如果荣誉不够分量的话，那么这些奖金应该可以成为那位虚构的年轻物理学家的动力了。

14

千年问题的想法来自于兰登·克莱（Landon T. Clay），他是一位来自波士顿的商人，通过购买股票市场上的共同基金发家。尽管在哈佛的时候他放弃了数学，但是他对这个领域有着一种热情，一种渴望参与的热情。他知道金钱不可能成为数学家的动力，“激励数学家前进的，是对真理的追求，以及对数学的优美、能力和精炼的感知”。但是克莱并不笨，作为一名商人，他知道100万美元可以使另一位安德鲁·怀尔斯加入到解决这些伟大未解问题的队伍中来。实际上，在发布问题后的第二天，刊登有这些问题的克莱数学研究所（Clay Mathematics Institute）的网站就因为点击数过多而崩溃。

7个千年问题在本质上不同于一个世纪前出现的那23个问题。希尔伯特实际上是为数学家制定了一份20世纪的行事日程。这些问题中有许多问题是有创造性的、能激发各自领域新观点的问题，而不是仅仅关注像费马大定理那样的单个问题。希尔伯特的23个问题使得数学界能从概念上思考问题。并不是单纯地挑出地面上的石块，希尔伯特提供给数学家各个领域的热气球，这样可以使他们在足够高的地方看到地面的全貌。这个新思想在很大程度上归功于黎曼，在50年前他将数学从一个仅仅考虑公式和方程的学科，转变为一门专注于思想和理论的学科。

但是新千年7大难题的选择就保守得多。比起希尔伯特那些现代的、先锋的选择，这些问题只不过是数学问题长廊中的经典问题。保守地选择这些新问题，其部分原因是，要评判提交人是否可以得到那100万奖金，那么其解答就应该有足够清晰的结构。这些问题都是数学家几十年来熟知的问题，特别是黎曼假设，它的历史已经超过一个世纪。所以这样的一个选择是经典的选择。





图4 法兰西学院

克莱为解决数学问题提供的700万美元奖金并非历史上的首次。在1997年，安德鲁·怀尔斯就因为证明了费马大定理而得到75000德国马克的奖金，那是一位叫保罗·沃尔夫斯凯尔（Paul Wolfskehl）的人于1908年设立的，当年正是沃尔夫斯凯尔奖的故事让10岁的怀尔斯知道了费马大定理。因此克莱相信如果自己能对黎曼假设做些什么的话，100万美金的投入是值得的。最近，两家出版社，英国的Faber & Faber和美国的Bloomsbury为哥德巴赫猜想设下100万美元的悬赏，用来推销阿波斯托罗斯·多克夏迪斯（Apostolos Doxiadis）的小说《佩特罗斯叔叔和哥德巴赫猜想》（*Uncle Petros and Goldbach's Conjecture*）。为了获得这笔钱，你必须说明为什么每个偶数都可以写成两个素数的和。不过，出版商并没有给太多时间，提交答案的截止日期是2002年3月15日，并且仅限美国和英国公民参加。

克莱认为数学家并没有获得与他们的付出相等的回报和认同。比如说，大家渴望得到的诺贝尔奖中不包括数学奖；取而代之，菲尔兹奖被认为是数学界的最高荣誉。不过，与诺贝尔奖往往是授予那些功成名就的科学家，以表彰他们长期以来取得的成就不同，菲尔兹奖仅限授予40岁以下的数学家。其中原因并非通常认为的，数学家的才能在早年就耗费殆尽。提出这个想法并提供基金的约翰·菲尔兹（John Fields）希望能通过这个奖，激励那些有前途的数学家做出更大的成就。菲尔兹奖于

每四年一次的国际数学家大会上颁发，其首次颁发是在1936年的奥斯陆。

非尔兹奖的年龄限制一直被严格遵守着。尽管怀尔斯证明了费马大定理，是一项非凡的成就，但是由于他出生于1953年，在他的最终证明被接受之后的1998年的国际数学家大会上，他还是不能获得菲尔兹奖。最后组委会只好设了一个特殊的奖项来表彰怀尔斯的成就，但这终究不能和成为杰出的菲尔兹奖获得者俱乐部成员相比。这些成员中有不少本书中的重要角色：恩里克·邦比艾里，阿兰·科纳，阿特勒·塞尔伯格（Atle Selberg），保罗·科恩（Paul Cohen），亚历山大·格罗腾迪克（Alexandre Grothendieck），阿兰·贝克尔（Alan Baker），皮埃尔·狄利津（Pierre Deligne）。这差不多占了所有得奖者的五分之一①。

数学家对奖项的渴望并非是为了奖金。和诺贝尔奖的巨额奖金相比，菲尔兹奖的奖金只有区区的15000加拿大元。因此克莱的100万美元绝对可以在金钱数上和诺贝尔奖相比，并且比起菲尔兹奖和Faber-Bloomsbury的哥德巴赫悬赏，它没有年龄限制，也没有国籍限制，更没有截止期限，除了通货膨胀导致的货币贬值。

然而，促使数学家去解决千年问题的最大动机并非是金钱上的回报，而是数学所能给予的令人心醉的不朽声名。解决一个克莱问题也许可以使你获得100万美元，但这又如何比得上将自己的名字镌刻在人类文明的智慧墙上呢？黎曼假设，费马大定理，哥德巴赫猜想，希尔伯特空间，拉马努扬 τ（Tau）函数，欧几里得算法，哈代-利特伍德圆方法，傅里叶级数，哥德尔计数法，西格尔零点，塞尔伯格迹公式，埃拉托塞尼筛法，梅森素数，欧拉乘积，高斯整数，等等。所有这些发现都是我们在探索素数时找到的宝藏，而发现它们的数学家也因此获得不朽的声名。即使我们忘记了埃斯库罗斯、歌德和莎士比亚，这些数学家的

---

① 截至2006年，获得菲尔兹奖的数学家一共有48位，其中包括了2006年拒绝领奖的俄罗斯数学家格里高利·佩雷尔曼。



名字仍将永远存在。正如哈代所说，“语言会死亡，可是数学的思想不会。‘不朽’也许不太恰当，但数学家是最适合它的含义了。”

这些为了理解素数而长途跋涉于数学世界中的数学家，并不仅仅是留下名字而已。素数故事的迂回曲折是由真实生活和生动丰富的角色构成的。法国大革命中的历史人物、拿破仑的朋友让步于当代的魔术大师、网络公司；加上来自印度的小职员、逃过死刑的法国间谍、以及一个逃过了纳粹德国迫害的匈牙利裔犹太人的故事，都因为素数的关系而联系在一起。所有这些角色都因为给该领域带来了独特视角而在数学史上留下印记。素数问题吸引了许多国家的数学家为之奋斗：中国、法国、希腊、美国、挪威、澳大利亚、俄罗斯、印度和德国只是产生过杰出数学家的一些代表。每四年数学家都会在国际数学家大会上聚集起来，讲述各自的故事。

数学家的动力并不仅仅是为了在历史上留下足迹。正如希尔伯特敢于正视未知，证明黎曼假设将标志着一段新旅程的开始。在发布克莱奖的当天，怀尔斯在会议上的演讲中强调了这些问题并非是最终目标：

> 有一个全新的数学世界等待我们去发现。想象一下，在1600年的欧洲，人们知道在大西洋的另一端有一个新大陆，那么应该如何设立一个奖项，来帮助这次探险，以及将来美国的发展？是设立发明飞机奖，发明计算机奖，发现芝加哥奖，还是发明收割机奖？虽然这些在今日美国已经实现，可是当时的人们却想象不到。他们所能做到的，就是设立一个奖，用来奖励解决经度问题的人。

17

黎曼假设就是数学的经度。解决了黎曼假设，就会为我们提供在浩瀚的数字海洋上标注模糊海域的机会。它代表的是我们理解自然数的开始，在我们发现了如何操纵素数的秘密之后，谁知道会有什么在那里等着我们去发现呢？

18

第二章

算术的原子

当问题变得过于复杂时，有时应该停下来想想：我是不是提出了正确的问题？

——恩里克·邦比艾里，《科学》杂志

邦比艾里的愚人节玩笑戏弄了整个数学界。在两个世纪之前，另一位意大利人古色佩·皮亚兹（Guiseppe Piazzi）从巴勒莫传出了一条同样令学术界兴奋的新闻。在他的天文台里，皮亚兹发现了一颗新的围绕太阳运转的行星，其轨道位于火星和木星之间，该行星被命名为谷神星[①]。它比当时发现的七大行星都要小，但在它被发现的1801年1月1日，所有人都认为该发现是新世纪科学的一个好兆头。

数个星期之后，兴奋转变为失望。当这颗行星运动到太阳另一侧的轨道之后，由于太阳的光芒掩盖了它微弱的星光，它消失在人们的视野中。此后它消失不见，再次藏匿到天空的群星之中。在19世纪初期，天文学家没有足够的数学工具，根据他们数星期观测到的短期轨道，计算出行星的完整轨道。看起来，人们已经丢失了这颗行星，并且不能预测它将出现在何处。

然而在皮亚兹的这颗行星消失快一年之后，一位24岁、来自不伦瑞克（Brunswick）的德国人宣称他知道天文学家在何处可以找到他们

---

① Ceres，以罗马神话中的谷物女神命名，因此称为谷神星。谷神星实际上是位于火星和木星之间小行星带中最大的一颗小行星。



丢失的行星。别无他法，天文学家将他们的望远镜对准了这位青年指出的那片夜空。令人惊讶的是，它竟然就在那里。这次空前的天文学预测并非是出自某位占星家的魔法，而是一位数学家计算出了谷神星的轨道。在别人只能看见一颗小小的行星的情况下，他却能发现其中的规律。卡尔·弗雷德里克·高斯（Carl Friedrich Gauss）在别人记录下的少量数据的基础上，利用他最近发展出来的新方法，成功地估计出在未来任何时间谷神星的位置。

发现谷神星的轨道令高斯成为科学界的一颗新星。在19世纪初，在即将到来的科学时代，他的成功标志着数学的预知能力。当天文学家还只能靠运气发现行星时，数学家已能运用相应的分析知识解释事物将如何发展。

19

尽管高斯这个名字对于天文学界是陌生的，但是他在数学界早就标志着强大的新声音。虽然他成功地计算出谷神星的轨道，但是他真正的激情是为了找出数字世界的规律。对高斯而言，只有在数的宇宙中才能找到终极挑战：从别人眼里的混沌中找出结构和规律。“神童”和“数学天才”这些名字虽然经常出现，但是如果这样来称呼高斯，几乎没有数学家会反对。这不需要解释，仅凭高斯在25岁之前提出的新思想和新发现的绝对数目就可以说明。

高斯1777年出生在德国不伦瑞克的一户农家。在3岁时他就能纠正父亲计算中的错误，在19岁时，他发现了一种优美的构造十七边形的几何方法，这个发现最终促使他投身数学。在高斯之前，希腊人已经知道如何利用圆规和直尺作出正五边形，但是没有人知道如何利用这两件简单工具作出具有素数条边的正多边形。在高斯找到作出正十七边形的方法后，兴奋的他决定开始记数学日记，并且在随后的18年里一直坚持这个习惯。这份在1898年之前一直保留在高斯家族的日记是数学史上最重要的文献之一，其原因并非它证实了那些高斯曾经证明但没有发表过的结果，而是因为它可以使得其他数学家重新回到19世纪去再发现。



高斯早期最重要的贡献是发明了时钟计算器（clock calculator）。这是一种思想，而不是一架机器，它使得曾经被认为不易操作的数的计算成为可能。时钟计算器像我们通常的时钟一样工作，如果钟面上显示现在是9点，那么加上4个小时后，时针将指向1点。高斯的时钟计算器的输出就是1而不是13。如果他想进行更复杂的运算，比如说7×7，那么时钟计算器将会给出49 =7×7被12除之后得到的余数，结果仍然是1。



图5　卡尔·弗雷德里克·高斯（1777~1855）

当高斯打算计算7×7×7时，这个计算器的威力就开始凸显了。这



次并不需要将 49 乘以 7，而是将上一个结果（也就是 1）乘以 7，就可以得到结果 7。因此无须计算 7×7×7 究竟等于多少（恰好就是 343），只要稍加计算也可以知道这个数被 12 除之后的余数是多少。当高斯开始考虑超出计算极限的数时，计算器终于显示出它真正的实力。尽管他不知道 7^{99} 是多少，但是计算器告诉他这个数被 12 除之后的余数为 7。

高斯发现时钟表面的时间刻度为 12 并没有什么特殊性，因此可以将这个时钟算法思想推广到任意数。比如说，在表面刻度为 4 的时钟计算器中输入 11，你可以得到 3，因为 11 除以 4 的余数就是 3。高斯的这种新发明是 18 世纪与 19 世纪交替时期数学领域中的革命，如同望远镜帮助天文学家看到了新世界，时钟算法的出现也帮助数学家发现了数之宇宙的新规律，而这规律曾历经数千年不见其踪。即使在今天，高斯的时钟计算器还是因特网安全的核心，不过这些时钟的刻度要比可观测宇宙中的原子数还要多。

作为出生在贫困家庭的孩子，高斯很幸运地得到了发挥数学才能的机会。在他出生的那个年代中，数学是由宫廷或贵族资助的特权活动，或者像费马一样在业余时间进行自学。高斯的资助人是不伦瑞克公爵卡尔·威尔海姆·费迪南（Carl Wilhelm Ferdinand），费迪南家族有着资助自己领地中文化和经济的传统，费迪南的父亲曾资助成立了卡罗林学院（Collegium Carolinum），这是德国最古老的技术学院之一。受其父影响，费迪南深知教育是不伦瑞克商业成功的基础，因此他总是在寻找那些值得资助的天才。费迪南在 1791 年碰见高斯后，立刻对高斯的才能留下深刻印象，于是资助高斯进入卡罗林学院，以便高斯能发挥所长。

心存莫大的感激，高斯将其于 1801 年出版的第一本书奉献给公爵。这本书名叫《算术探讨》（*Disquisitiones Arithmeticae*），收集了高斯曾经记于日记中的那些有关数的性质的结果。普遍认为，该书标志着数论正式成为一门学科，而非搜集那些有关数的性质的破布袋。它的出版也标志着数论成为高斯所说的"数学的皇后"。对高斯而言，素数就是皇冠上镶嵌的宝石，数代的数学家在为这些宝石倾倒的同时也因其而

烦恼。

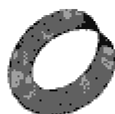
现今所知的人类最早尝试了解素数的证据是一块公元前6500年的骨头。这块骨头被称为伊山沟甲骨（Ishango Bone），它于1960年在赤道中非的一座山上被发现。在它上面刻着三列四组刻痕，其中一列有11、13、17、19个刻痕，这正是10到20之间的所有素数。其他两列看起来更像是数学天性的体现。现在并不清楚，这块现藏于布鲁塞尔比利时皇家自然科学院的骨头，是否真的表示我们的祖先首次尝试去了解素数，还是只是随机选择出来，恰好构成一列素数。但是无论如何，这块祖先的骨头也许正是人类首次进攻素数理论的证据。

22

有人认为中国人是最先听到素数心跳的民族。中国人将雌性特征归为偶数，雄性归为奇数，并且除了如此直接的划分之外，他们还认为那些非素数的奇数，比如说15，是具有女人气的数。有证据表明在公元前1000年，中国人就能够从物理观点理解在所有的数中，为什么素数是如此的特殊。如果你有15个豆子，你可以很容易地将它们排成一个长方形，三行五列。但是如果你有17个豆子，你能唯一排成的长方形就是一行。对中国人而言，素数就是具有男子气的数，它们抵抗着任何试图将它们写成两个更小的数之乘积的尝试。

古希腊人也愿意给数附上性别的含义，但他们首先于公元前4世纪发现，素数真正的实力在于它是构成所有数的基石。他们发现，所有的数都可以通过将素数相乘得到。虽然古希腊人错误地认为火、空气、水和泥土是构成世界万物的原子，但他们在辨认算术的原子这个问题上却得到了正确的结果。许多世纪以来，化学家为了鉴别出自己学科中的基本元素而努力。最终，迪米特里·门捷列夫（Dmitri Mendeleev）的元素周期表终结了希腊人的直觉，这是对化学元素的完整描述。尽管古希腊人早已发现了构建算术世界的基石，但是数学家仍在为了理解素数表而奋斗。

现今我们所知最早编制素数表的人是一位图书馆员，他任职于亚历山大的古希腊最高研究所。作为古代的数学界的门捷列夫，埃拉托塞尼



（Eratosthenes）于公元前3世纪发明了一种合理的、不复杂的方法，来辨认出一张表（比如说前1000个数）中的数是否为素数。首先把1到1000这些数依次写下来，取第一个素数2，并将表中的每第二个数划去，因为这些数能被2整除，所以不是素数；然后找到第一个未被划去的数，也就是3，因此表中每第三个数也将被划去，因为它们能被3整除，所以不是素数。如此这样做下去，只需挑出没有被划去的第一个数，再划去之后那些能被该数整除的所有数，由此过程我们就可以得到一张素数表。这个过程后来被命名为埃拉托塞尼筛法，每一步产生的新素数都可以生成一张筛，埃拉托塞尼利用它们删去那些非素数。每一步筛的大小都在变化，当到达1000之后，那些能通过所有筛的数就是素数。 23

当高斯还是小孩时，他收到一份礼物：一本含有前数千个素数表的书，这些素数很有可能是利用古代的筛法得到的。在高斯的眼中，这些数完全是随机出现的。预测谷神星的椭圆轨道已经很不容易，但是素数带来的挑战则像研究汉堡状的土卫七①的不规则旋转一样，是接近于不可能的任务。与地球的卫星月球不同，土卫七不能在引力作用下保持稳定，并且无规律地旋转。即使土卫七的旋转和其他小行星的轨道是如此不规则，至少我们知道这些行为是太阳和大行星引力共同作用的结果。但是对于素数，对于究竟是什么令素数出现在这里而不是那里，人们连最简单的想法也没有。当凝视这些素数表的时候，高斯看不出任何规则能告诉他究竟隔多远找到下一个素数。是不是数学家就应该接受这个事实，即这些素数是由大自然决定，如同天空中的繁星一般没有任何规律和理由？高斯无法接受这样的处境。数学家的原动力就是找出事物之间的规律，发现和解释隐藏在大自然之下的规律，预测未来将会发生什么。

---

① Hyperion在希腊神话中是大地女神盖亚和天王乌拉诺斯之子，是太阳神之父，天文学上用来命名土卫七。土卫七是土星已知卫星中离土星第十六近的卫星，于1848年被发现，它是太阳系中最大的一颗高度不规则（非球形）天体，也是太阳系已知星体中唯一一颗自转混乱的星体。

寻找规律

数学家对素数的研究，可以用一个我们在学校中经常碰到的问题来完美地说明。给定一列数，找规律写出下一个数。比如下面的三个问题：

1，3，6，10，15，…

1，1，2，3，5，8，13，…

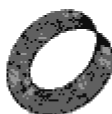
1，2，3，5，7，11，15，22，30，…

当看到这些数列时，数学家脑中会出现许多问题：生成这一列数的背后规律是什么？你能预测下一个数吗？你能找出一个公式，不用计算前99个数，就可以写出第100个数是多少吗？

上面的第一列数由所谓的三角形数组成。这列数中的第十个数等于一个由十行豆子组成的三角形中的豆子数：第一行放一个豆子，最后一行放十个豆子。因此第 N 个三角形数就是简单将前 N 个数相加：$1+2+3+\cdots+N$。如果你想找到第100个三角形数，你将面对的是将前100个数相加这样的苦干。

不过，高斯的老师确实喜欢在课堂上将这个问题留给学生，这样在学生们努力计算的过程中，他可以小睡一下。在每个学生都完成了他们的计算之后，他们需要将结果写在计算板上交到老师的面前。正当其他同学都在辛苦计算时，10岁的高斯很快就交上了他的石板。面对这样无礼的行为，老师感到非常愤怒。但是当他看到高斯的石板上面写着正确答案5050，而没有任何过程的时候，他认为高斯肯定是偷看了结果。最后高斯解释说，只需要将 $N=100$ 代入公式 $\frac{1}{2}\times N\times(N+1)$，就可以不用计算其他任何数，而直接得到这第100个数。

在此高斯并没有直接逐个计算，而是从侧面解决了这个问题。他指出，找出一个100行的三角形中所含的豆子数的最好方法，就是取另外



一个相等的三角形，头尾倒置放在第一个三角形旁边。这样我们就得到一个 101 行的长方形，每一行有 100 个豆子。计算这两个三角形组成的长方形中的豆子数是很简单的，就是 $100\times101=10100$ 个豆子。因此每个三角形所含的豆子数就是该数的一半，也就是 $\frac{1}{2}\times100\times101=5050$。由于这里的 100 并不特殊，因此将它替换为 N 就可以得到公式 $\frac{1}{2}\times N\times(N+1)$。

图 6 表示了 10 行的三角形数的计算。

并非直接计算老师给出的问题，高斯找到了另外一个计算的角度。横向思维，就是将问题上下翻转或里外调换，以获得一个新的观察角度。它是数学研究中一个极其重要的方法，也是那些可以像年轻高斯一样思考的人能成为数学家的原因。

第二个具有挑战性的序列，1，1，2，3，5，8，13，…被称为斐波纳契数列。这个数列背后的规则是，每一个数都是前面两个数之和，比方说 $13=5+8$。莱昂纳多·斐波纳契（Leonardo Fibonacci）是 13 世纪比萨的一位宫廷数学家，他在研究兔子的繁殖问题时碰到了这个数列。他曾经想用阿拉伯数学把欧洲数学从黑暗时代中解脱出来，不过他失败了。但是，兔子问题使他永远留名于数学界。从他关于兔子繁殖的模型可以看出每一年兔子个数①的增长满足一定模式，这个模式基于两条规则：每一对成熟的兔子在一年中只生育一对小兔子；每一对小兔子需要一年时间达到性成熟。

25

但是这些数并非只在兔子世界起作用。这些数自然地出现在各个地方，花瓣的个数是斐波纳契数，松果上的螺旋数也是斐波纳契数，海贝的生长同样反映着斐波纳契数。

如同高斯的三角形数公式，是否有一个公式可以快速地计算出第 100 个斐波纳契数？初看上去，我们必须计算前 99 个数，因为计算第

① 这里是以一对兔子为计数单位。



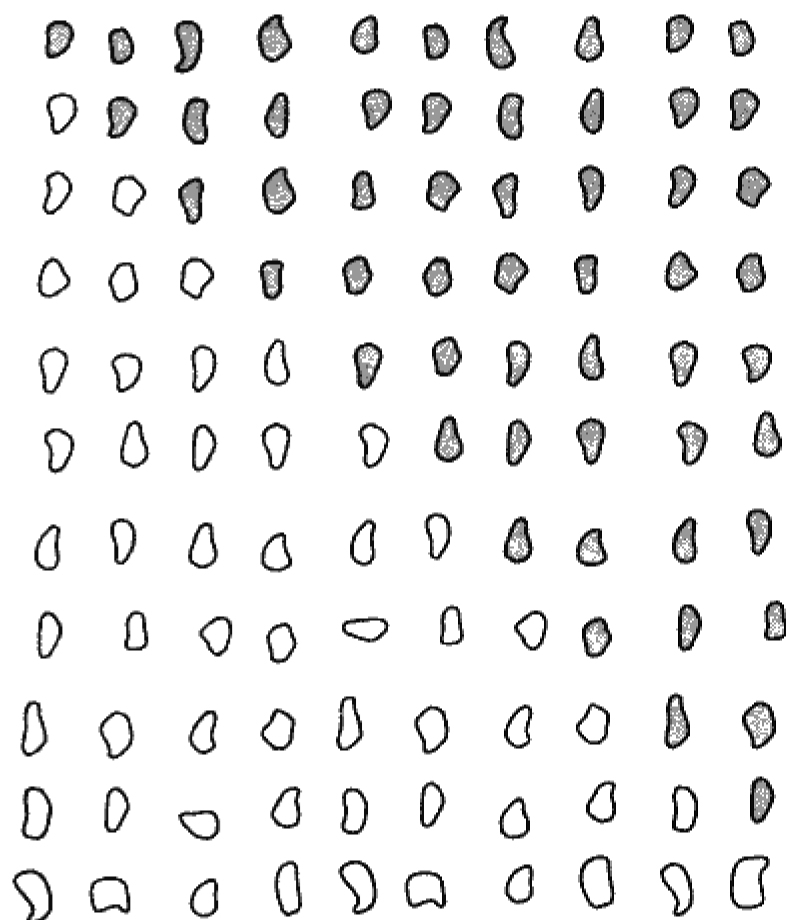


图 6　高斯关于三角形数公式的证明的示意图

26

100 个数的方法就是将第 98 个和第 99 个数相加。那么是否有一个公式，我们只需将 100 代入，就可以计算出第 100 个斐波纳契数？虽然生成斐波纳契数列的规则很简单，但是想要得到这个公式却需要不少技巧。

生成斐波纳契数的公式基于一个特殊的数——黄金比例，它的开头几位是 1.618013…与 π 一样，黄金比例具有无穷位的十进制展开，并且毫无规律，但是从古至今它就被当作是完美比例的代表。如果你看过卢



浮宫或泰特美术馆①中的那些画布，你会发现画家们通常都会选择长宽比为1：1.618013…的长方形。实验表明人体的高度相比于从肚脐到脚的距离同样是这个比例，黄金比例数就是以如此神秘的方式出现在自然界中。抛开它无规则的小数展开，这个数同样掌握着生成斐波纳契数列的关键，第 N 个斐波纳契数是由一个含黄金比例的 N 次幂的公式生成。

我将第三列数1，2，3，5，7，11，15，22，30，…先留作给读者的挑战，稍后我会回来谈它。它的性质与20世纪最神秘数学家斯尼瓦萨·拉马努扬（Srinivasa Ramanujan）的盛名紧密相连。拉马努扬拥有超常的能力，他能够找出那些别人尝试过但却没有发现的规律和公式。

在自然界中并非只能找到斐波纳契数，动物世界也知道素数。有两种生活在同一环境的蝉分别叫做十七龄蝉和十三龄蝉，它们的生命周期恰好就是17年和13年。除了最后一年，它们都是深藏于地下吸食树根的汁液，到了最后一年，它们全部从地下出来，蛹化为成虫。对十七龄蝉而言，经历了17年的长夜，这就是一个特殊的时刻。它们大声的鸣叫、交配、进食、产卵，然后在6个星期内死去。此后森林又将经历17年的寂静。但是为什么这些物种选择一个素数作为它们的生命周期呢？

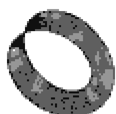
这里有几个可能的解释。首先，由于这两个物种的生命周期为素数，它们不太可能于同一年离开地下。实际上需要 $221 = 13 \times 17$ 年的时间，它们才有可能同年出现于地面。假设它们不是选择素数年为周期，比如说18和12，那么在同样的时间内，它们会相遇6次，即第36、72、108、144、180和216年，因为这些年与18和12共享那些素数因子。这样看来，素数13和17，就使得这两种蝉避免了过多的竞争。

27

另外一种解释是，有一种真菌与蝉同时生长，而这种真菌对于蝉是致命的，因此蝉需要进化出一个生命周期来躲开真菌。通过进化为13和17这样的素数周期而不是其他非素数周期，蝉可以保证与这些真菌相遇在同一年的几率最小。对蝉而言，这些素数并非抽象的巧遇，而是

---

① 位于英国伦敦的现代艺术馆。



它们生存的关键所在。

尽管进化理论可以解释蝉生命中的素数问题，数学家仍希望能有一个更系统的方法来找到这些素数。在所有的数论问题中，寻找素数表的秘密公式最重要。但是需要注意，数学世界中并非处处都有模式和规律。就数学中最重要的数 π 而言，在历史上曾有许多人因为试图寻找它的十进制小数展开中的结构而迷失，但是 π 的重要性却不断地激发着那些无望的尝试。在萨根的小说《接触》的开头，外星人利用素数吸引了伊莉·阿若薇的注意力。达伦·阿若诺夫斯基（Darren Aronofsky）的电影《π》同样反映了这一流行文化特征。

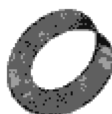
在此我要劝告那些迷恋于试图揭开诸如 π 的数的背后信息的人，数学家已经证明，在它们的无穷展开中，你可以找到那些你想寻找的绝大多数十进制数。因此，如果给你足够长的时间进行搜索，你有很大的机会在 π 中找出《创世记》的计算机编码。因此我们需要找到一个正确的观察角度来寻找数字背后的规律。π 的重要性并非仅仅因为它的十进制展开中存在着隐藏信息，只要你换一个角度它的重要性就会显现。素数也是如此，利用素数表及横向思考的能力，高斯得以从正确的角度和观点来审视素数，从而发现某些潜在的规律，而这些规律正是隐藏在表面的混乱之下。

28

证明：数学家的旅行日记

找出数学世界的规律和结构，只是数学家的一半工作；另一半工作是证明这些规律确实存在。证明的出现也许标志着数学作为演绎推理艺术而不是数字观测结果的真正开始，正是在这一点数学世界中的炼丹术让位于化学。古希腊人最先明白，如果能够证明某个结论，那么无论你数到多大，也不管你验证多少实例，这个结论将始终成立。

数学创新的过程从猜测开始。通常，猜测来自数学家的直觉。凭着多年在数学世界中的探索，数学家逐渐形成一种感觉，能够感知许多关



键的所在。有时简单的数字计算就能发现一些规律，并可以随之猜测其永远成立。比如说，17 世纪的数学家自认为他们发现了一种万无一失的测试某数 N 是否为素数的方法：计算 2 的 N 次方，然后除以 N，如果余数为 2 则说明 N 是素数。用高斯的时钟计算器语言来说，这些数学家试图在表面为 N 的时钟上计算 2^N。此时的挑战就是证明该猜测正确与否。这些数学界的猜测或预言就是数学家口中的"猜想"或"假设"。

只有得到了证明，数学猜测才能获得"定理"之名。正是这个从"猜想"或"假设"到"定理"的过程，标志着数学作为一门学科的成熟。费马留给了数学界一大堆预言，此后数代数学家通过证明费马预言的正确或者错误而成名。不可否认，费马大定理一般被称为是定理而不是猜想。但是这种情况并不多见，也许是因为费马在丢番图（*Diophantus*）的《算术》（*Arithmetica*）一书上写下的潦草的注记，声称他已经找到了一个不可思议的证明，只是由于证明太长而无法在书的页边空白处写下。由于费马没有在别的地方记录这一所谓的证明，因此他在书页上的注释也成为了数学界最大的烦恼。在怀尔斯证明了费马的方程确实没有正整数解之前，费马大定理实际上只是一个猜想，所谓的定理只是人们的主观愿望。

高斯的教室插曲生动地表现了从猜想经过证明到定理的过程。高斯发现了一个公式，并预言它可以生成任意的三角形数。他是如何保证这个公式每次都有效呢？他当然不可能检验每一个数，来验证该公式是否给出正确结果，因为这是一个无穷过程。他利用的强力武器就是数学证明。他通过拼凑两个三角形得到一个长方形的方法保证了该公式的有效性，而无须经过无穷多次验算。作为对比，17 世纪的基于 2^N 的素数检验法，最终在 1819 年被逐出数学世界。该方法对于 340 以内的数均有效，但是它判断 341 是素数。正是这一点使得该方法失效，因为 $341 = 11 \times 31$。这个反例直到高斯的时钟计算器出现之后才被发现。利用刻度为 341 小时的时钟计算器就能简化计算 2^{341} 这样的数，因为在通常的计算器上它的长度超过了一百位。

29



《一个数学家的自白》的作者，剑桥的数学家哈代常喜欢用给遥远景物绘图，来描述数学发现与证明的过程："我常想，一个数学家首先应该是一个观测者，他凝视着远方群山的轮廓并记录下他观测到的一切。"一旦数学家观察到了一座遥远的山丘，那么第二件事就是告诉人们如何到达那里。

你出发的位置，其风景是熟悉的，没有任何惊奇。在这片熟悉土地的边界之内，是数学中的公理、那些关于数的不证自明的事实、还有那些已经被证明的命题。证明就像是从家园出发，穿过数学世界，直到远方山顶的道路。由推理规则界定的过程，就像是象棋中的正确步骤，规定着你在这个世界中被允许走的那些地方。有时，你会碰到僵局，此时你需要特别的迂回战术，向旁边移动甚至是后退几步，来寻找另外的道路。有时你则需要等待新工具的发明，像高斯的时钟计算器，你才能继续你的攀登。

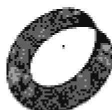
用哈代的语言，数学观测者

> 可以清晰地看见A，但只能时不时地看见B。最终他辨认出一条从A出发的山脉，沿着它走到终点，他发现终点就是B。如果他希望别人也能看到这条山脉，他可以直接指出它，或者指出那一系列曾引导自己到达终点的山峰。当他的学生也能看到这一切的时候，研究工作、论证和证明也就结束了。

30

证明是探险故事，是旅程中标明坐标的地图，也是数学家的日志。在证明中读者能体会作者思想的起源。读者不光可以看见最终通往顶峰的道路，而且他们知道新的发展也无法影响已有的道路。很多时候证明不需要详细到每一个细节，它只是对路程的描述，没有必要对每一步都加以规定。数学家提供的证明，应该是经过设计的、可以促使读者思想飞跃的论证过程。哈代曾将我们所谓的论证描述为"火上的油，影响他人心理的华丽辞藻，课堂黑板上的示意图，激发学生想象力的东西"。

数学家对证明是如此着迷，因此对某个猜想不可能简单地相信一些



实验证据。在其他学科中，这种态度常常被认为是奇怪甚至是可笑的。已经验证在400 000 000 000 000以内，哥德巴赫猜想都是正确的，可是它仍然不能成为定理。大部分的科学学科会很高兴地接受如此具有说服性的数字，并将它作为令人信服的论证，然后着手其他的工作。即使以后出现了新的证据，需要对这个数学准则进行再评价，那也是可以的。如果别的科学都可以这样，为什么数学一定要特立独行呢？

大部分数学家对如此的异端想法都会气得浑身发抖。法国数学家安德烈·魏伊（André Weil）说过，“严格性对数学家而言，就如同人类的道德一样（重要）。”部分原因是事实证据在数学中难以评价，相比其他数学内容，素数需要更长的时间来显现出本色。在判断他关于素数的一个猜测时，即使是高斯也轻信了那些具有说服力的数据，但是后来的理论分析证实高斯被数据所欺骗。当其他学科信奉实验证据就是一切的时候，数学家就已认识到永远不能相信缺少证明的数据。

某些观点认为，作为一门心智学科，数学精神上的本质使得数学家更多地依赖于证明提供的对于这个真实世界的感觉。化学家可以兴奋地探索真实的富勒烯分子①，基因排序则是遗传学家面前的一项具体挑战，甚至物理学家都能感觉到最微小的亚原子粒子或者遥远黑洞的存在。数学家面对并试图理解的那些对象根本就没有明显的物理实在，像八维空间中的形状、那些比所有物理宇宙中原子数还要大的素数。对于给定的抽象概念，思想可以对其施展新奇的技巧，但如果缺少证明，这一切就只能是空中楼阁。在其他学科中，有形的观测和实验为物体的存在提供了某种程度的保证。当其他学科的科学家亲眼看到这些物理实在的时候，数学家只能依靠类似第六感觉的数学证明与这门不可见学科进行交流。

31

---

① Fullerene，全名 buckminster fullerene，又名巴基球或巴克球（Buckyball），是于1985年发现的继金刚石和石墨之后碳元素的第三种晶体形态。它是由60个碳原子以20个六元环和12个五元环连接而成的具有30个碳碳双键（C＝C）的足球状空心对称分子，所以，富勒烯也被称为足球烯。



寻找那些已经显现的规律的证明，同样也是数学发现的催化剂。许多数学家认为，如果这些问题永远得不到解决，结果将更好，因为一路上总是会碰到奇妙的新数学领域。在探索旅程中，数学先锋探索的领域，是他们在开始旅程时完全没有想到的领域。

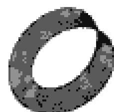
为什么数学文化是扎根于证明一个命题的真假之上？也许对此最令人信服的解释是，能够从事数学而不是其他学科，是一件很荣幸的事。有多少其他的学科，在其中能够找出像高斯的三角形数公式那样永远不会失效、总是能给出正确答案的命题呢？数学也许是一门被囿于头脑中的非物质学科，缺少可触及的实体，但是证明提供的确定性恰恰就是对此的补偿。

其他学科中的世界模型也许在两代之中就会崩溃，但是数学中的证明可以让我们百分之百地相信，现在有关素数的事实，在未来新发现的再验证之下仍然保持正确。数学就是一座金字塔，每一代人在上一代人的成就之上进行建造，无须担心任何倒塌的危险。这种持久性也正是数学家沉溺其中的原因所在。除了数学之外的任何学科，我们都不能说那些古希腊人建立的理论至今仍然适用。古希腊人曾经认为物质是由火、空气、水和泥土组成，今天我们认为这是笑谈。也许未来的后代们，在看到门捷列夫元素周期表中109种原子时候的表情，就和我们现在回看古希腊的化学世界模型时的表情一样。与之形成鲜明的对比，古希腊人证明的那些关于素数的理论，仍旧是今天所有的数学家在开始他们的数学教育时所要学习的东西。

证明给予数学家的确定性，在被大学里其他院系成员嘲笑的同时，也被同样多的人嫉妒。数学证明创造出来的持久性导致了哈代所说的永恒。这也是为什么被不确定世界包围的人们会被这门学科吸引的原因。长期以来数学世界为那些年轻的、渴望从这个他们无法应付的世界逃脱的人提供了一个避难所。

32

我们对于证明持久性的信心同样体现在克莱千年大奖的规则之中。只有在证明正式发表两年，并且被数学界普遍接受之后，才会授予奖



金。当然，这仍然无法避免其中存在的微小错误，只是人们普遍认为即使存在这样的错误，那也是已经被标注出来了，而无须等待多年的新证据。如果存在着错误，那一定是在我们面前的证明中。

是否数学家就是如此自大，认为自己掌握了通往绝对证明的道路？"所有的数都是由素数构成"这样的命题，有可能像牛顿物理理论，或者不可分原子理论那样被推翻吗？大部分数学家相信：这些有关数的不证自明的公理，在未来的审视下永远不会被推翻；建立于这些公理基础之上、正确应用逻辑理论而证明的有关数的理论，同样也不可能被新的观点推翻。也许这只是哲学上的天真，但这确实是数学分支的中心原则。

数学家在标注穿越数学领域的新道路时同样也会感受到兴奋之情。对于那些已经被数代人观测到的山峰，如果能发现某条通往该山峰的道路，所获得的感觉将是一种神奇的愉悦。这就如同想出了一段精彩的故事或音乐，能如实地将自己熟悉的思想传达给那些不知道的人。能第一眼看到那些遥远山峰——例如费马大定理或黎曼假设——当然很了不起，但这始终无法与指出两地之间联系的感觉相比。甚至那些沿着先驱足迹跋涉的人也能感受到某种精神上的、不亚于发现一个新证明的提升。这也是为什么数学家即使完全相信黎曼假设的正确性，却仍然如此重视对证明的追求。因为数学家不光重视终点，同样重视过程。

那么数学是一种创造的行为，还是一种发现的行为呢？许多数学家感觉自己的工作是创造性的，但是又无法排除这种感觉，就是他们只不过是在发现绝对的科学真理。数学思想经常出现在某个特定个人身上，并依赖于那些能感知它们的创造性思想。然而还有一种信念与之平衡，就是数学思想的逻辑特征意味着，所有的数学家都是生活在同一个充满永恒真理的数学世界中。这些真理只是简单地等待着被发现，没有任何创造性的思想可以破坏它们的存在性。哈代将这种位于创造性和发现性之间的、每一个数学家都曾经历过的紧张关系完美地概述为："我相信数学实在存在于自我之外，我们的作用就是去发现并观察它。我们证明

33



的那些定理，以及我们自豪地认为是我们‘创造’的东西，只不过是我们的观察记录而已。”但是在其他场合，哈代却更喜欢另一种更加艺术性的有关做数学过程的描述：“数学并非冥想，而是一门创造性的学科”，他在《一个数学家的自白》中这样说道。这本书与亨利·詹姆斯（Henry James）的笔记一起被格拉汉姆·格林（Graham Greene）认为是最好的描述创造性艺术家的书籍。

尽管素数以及其他一些数学分支，超越了文化的障碍，但是大部分的数学还是创造性的，是人类心智的产物。证明——数学家用来讲述他们学科的故事——也同样可以有不同的表述方法。很有可能怀尔斯关于费马大定理的证明对于外星人而言就像是听瓦格纳的《指环》一样神秘。数学是一门有限制的创造性科学，如同写诗或演奏布鲁斯音乐。由于逻辑规则的限制，数学家必须精心雕琢他们的证明。然而在这些限制之中，仍然存在着大量的自由。在限制之下进行创造性工作的美妙之处在于，你有时会被迫走向新的方向，并因此发现了那些你从没预料过你会独自发现的结果。素数如同音乐中的音符，不同的文化可以用其独有的方式来演奏这些音符，展现了意想不到的历史和社会的影响。素数的故事展示了对永恒真理的发现，同样也是反映社会的镜子。17 和 18 世纪对机器急速增长的热爱反映在素数领域是非常实际的、实验性的发展；而大革命时期的欧洲则弥漫着一种新气氛，全新的、抽象的以及大胆的思想被引入，全然不顾分析基础。如何选择穿过数学世界的道路，体现了这些不同的文化。

欧几里得的故事

最先讲述素数故事的是古希腊人。他们认识到，证明的力量足以铺设数学世界中通往高峰的永恒之路。一旦到达，就无须担心这些高峰只是遥远的数学幻想。比如说，为何我们能如此确信不存在一些无赖的数，它们不能通过素数相乘得到？希腊人提出的论证，不仅使他们自



己，同样也使未来的后代们确信，这样的无赖数不可能存在。

数学家寻找证明的过程，通常是对要证明的一般理论找出某个特例，进而理解为什么理论对这个特例而言是正确的。他们希望得到的论述或方法对所有的例子都适用，而与原先取来进行分析的特例无关。比如说，我们要证明每个数都可以写成素数的乘积，可以从取定一个特殊数 140 开始。假设你已经检验了 140 以下的数，它们或者是素数，或者可以写成素数的乘积。那么 140 本身又是如何呢？它会不会是一个既不是素数也无法写成素数乘积的无赖数？首先，你会发现 140 不可能是一个素数。如何证实？将 140 写成两个较小的数的乘积就可以。比方说 $140 = 4 \times 35$，此时我们就已经成功。因为在之前我们已经证实了 4 和 35，作为比 140 小的数，可以写成素数的乘积，即 $4 = 2 \times 2$，$35 = 5 \times 7$。综合起来，我们就得到 140 实际上是如下的一个乘积：$2 \times 2 \times 5 \times 7$，因此 140 不是一个无赖数。

希腊人懂得如何将这个特例的论证推广到一般情况，从而对所有数都适用。只不过，他们的论证要事先假定存在这样的无赖数——它既不是素数也不能写成素数的乘积。如果真存在这样的无赖数，那当我们按顺序数数的时候，肯定能碰到第一个无赖数，我们称之为 N（有时被称为最小罪犯）。既然 N 不是素数，那么它一定可以写成两个较小的数 A 和 B 的乘积，否则 N 一定是素数。

由于 A 和 B 都小于 N，并且由于我们的选择，N 是第一个无赖数，因此 A 和 B 一定可以写成素数的乘积。如果我们将由 A 和 B 分别得到的素数因子相乘，则一定可以得到原来的数 N。这样我们就证明了 N 一定可以写成素数的乘积，这与原先的假设矛盾。所以只能是原先的假设不成立。因此每个数或者为素数，或者由素数构成。

35

当我对朋友讲述这个证明的时候，他们的感觉是我在某一步要了花招。确实，这样的前提假设有点不可靠：先假设那些你希望不存在的东西存在，最后证明它们确实不存在。这种想人之不能想的策略是希腊人证明中的一件强有力武器。它依赖于如下的逻辑事实：一个命题非真即



假。如果我们假设命题为假，但是我们得到了矛盾，则可以推断出我们的假设错误，从而该命题一定为真。

希腊人的证明正表明了数学家的某种懒惰心理。无须正面迎击那些不可能的任务——对无穷多个数进行精确的计算来证明它们确实由素数构成，只需这种抽象的论述就可以抓住计算的本质。这就如同知道如何去爬一个无穷长的梯子一样，并不需要我们亲力为之。

在众多古希腊数学家中，欧几里得被认为是证明艺术之父。他任职于亚历山大城的研究机构，该机构由希腊国王托勒密一世于公元前300年前后建立。在那里，欧几里得写出了历史上最有影响的教科书《几何原本》。在这本书的第一部分，他选定了一些几何中用来刻画点线关系的公理，这些公理是作为不证自明的关于几何体的真理而给出的。这样几何就成为现实世界的数学描述，随后欧几里得利用推理规则证明了500个几何定理。

欧几里得的《几何原本》的中间部分，处理的是数的性质。正是在这里，我们找到了公认为是数学推理中第一个真正光辉的顶点。在命题20中，欧几里得解释了一个简单但却基本的关于素数的事实：存在无穷多的素数。他的出发点是如下事实，所有的数都可以通过素数相乘得到。在此基础上，他构造了接下来的证明。欧几里得自问，如果素数是所有数的构造基石，那么只存在有限块基石，可能吗？门捷列夫建立的化学元素周期表，直到现在仍然只包含了109种元素，但是却能由此组成整个物质世界。对素数会有同样的情况吗？假如也有一位数学界的门捷列夫给了欧几里得一份包含109个素数的清单，欧几里得是否能证明这个表中遗漏了某些素数？

为什么所有的数无法简单地由2、3、5、7的不同组合相乘构成？要证明这一点，只需找出那些不能由这些素数构成的数。一般人也许会说，“这很简单，只需要取下一个素数11就可以。”11显然是不能由2、3、5、7构造出来。欧几里得肯定也如此想过，只不过这个方法迟早会失效。因为直到今天，我们仍没有线索可以保证我们在哪里能找到下一





图 7　欧几里得，约公元前 350 ~ 前 300 年

个素数。由于这种不可预测性，欧几里得不得不寻找另外一种方法，一种不论素数表多长仍能适用的方法。

这究竟是欧几里得自己的想法，还是亚历山大的其他研究者的思想，欧几里得仅仅是将其记录下来，我们不得而知。但是不管怎样，他确实给出了一种方法，可以构造下一个素数，这个素数不能由其他有限素数表中的素数构成。取素数 2、3、5、7，欧几里得将它们相乘得到 2



×3×5×7=210，然后（这是天才思想所在）在此乘积上加1得到211。如此构造出的数211，它不能被素数表中的2、3、5、7整除，因为通过加1，可以保证所有除法的结果都将余1。

现在，欧几里得知道所有的数都是由素数相乘得到，那么211又如何？由于它不能被2、3、5、7整除，因此一定存在某个不在素数表中的素数构成了211。在这个特例中，211本身就是素数。欧几里得并没有证明，这样构造出的数一定是素数，他只是告诉我们，这个数是由一个不属于素数表的素数构成。

举例说，如果某人宣称所有的数都可以由有限素数表2、3、5、7、11和13构成。由这些素数构成的欧几里得数就是2×3×5×7×11×13+1=30031。这个数就不是素数。欧几里得所说的就是，给定任意的包含有限个素数的表，他可以构造出一个数，这个数是由不属于该素数表的素数构成。在这个特例中，找到的素数是59和509。但是一般而言，欧几里得无法知道如何去找出这些素数的确切值，他所知的就是这些素数一定存在。

这是一个绝妙的证明。尽管欧几里得不知如何准确地生成素数，但是他能证明为什么素数是无穷尽的。至今我们仍无法知道是否有无穷多个欧几里得数是素数，虽然通过它们可以证明存在着无穷多个素数。有了欧几里得的证明，我们就无法再期望存在着一个包含所有素数的周期表，或者是找到某种素数基因，通过它们可以生成无穷多的素数。简单的搜集并不能让我们理解这些素数。因此这就是终极挑战：拥有有限武器的数学家，位于无穷扩张的素数领域，是否可能标注出一条穿过如此混乱的世界的道路，并找出某些能预测它们行为的规律呢？

搜寻素数

此后的数代人一直在为了进一步深化欧几里得对素数的理解而努力，但是都失败了，不过其中倒是有一些有趣的结论。剑桥教授哈代常



爱说，“关于素数，普通人都可以提出一些最聪明的人也无法解决的问题。”比如说双生素数猜想①，问是否存在无穷多的素数 p 使得 $p+2$ 也是素数。其中的一对是 1 000 037 和 1 000 039。（注意，这是两个素数所能允许的最近距离，因为 N 和 $N+1$ 肯定不能同时为素数——除了 $N=2$——其中有一个肯定可以被 2 整除。）不知道萨克斯书中患有自闭症的天才双胞胎②对于找到这类的双生素数有没有特殊的天赋？欧几里得在 2000 年前证明了存在无穷多个素数，但是没有人知道是否存在这样的数，在它之外不存在如此接近的素数。不过我们相信存在着无穷多的双生素数。猜想终归是猜想，证明才是最终目标。

38

数学家曾经尝试找出某些公式，即使不能生成所有的素数，最起码能产生一系列的素数。这些努力取得了不同程度的成功，费马是其中一员。费马猜想对 2 作 2^N 次方并加一，那么结果 $2^{2^N}+1$ 是一个素数。这个数被称为第 2^{2^N} 个费马数。比如说当 $N=2$ 时，对 2 作 $2^2=4$ 次方，则得到 16，16 加 1 就是素数 17，这就是第二个费马数。费马认为这个公式总是能给出素数，但是它成为费马为数不多的失败猜测之一。费马数增长得非常快，第五个费马数就有 10 位，这超出了费马的计算能力，同时这也是第一个非素数的费马数，它能被 641 整除。

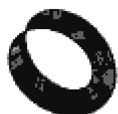
费马数深得高斯的珍爱。17 作为费马数的事实，正是高斯能够作出他完美的十七边形的关键所在。在他的巨著《算术探讨》中，高斯说明了，如果第 N 个费马数是素数，那么你可以仅用直尺和圆规作出 $2^{2^N}+1$ 边形的几何构造。第 4 个费马数为 65 537，它也是素数，因此可以用尺规作出一个完美的 65 537 边形。

费马数在给出了 4 个素数之后便失效了，但是费马在揭示其他有关素数性质的方面仍然取得了成功。他发现一个奇怪的性质，那些被 4 除之后余数为 1 的素数——比如说 5、13、17、29 等，总是可以写成平方

---

① The Twin Primes Conjecture，也称为孪生素数猜想。

② 这里作者利用了双胞胎的英文 twins 与双生素数猜想中的 twin 的对应关系。



和的形式，像 $29=2^2+5^2$。这同样是费马的一个挑战，尽管他宣称找到了证明，可是他没有写下更多的细节。

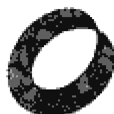
在 1640 年的圣诞节，费马将这个发现——某些素数可以表示成平方和的形式——写在信中，寄给了一位法国修道士马林·梅森（Marin Mersenne）。梅森的兴趣不光局限于宗教事务，他热爱音乐，并且是第一位发展和声理论的人，同时他也热爱数字。梅森与费马定期通信交流各自的数学发现，因此梅森将费马的许多发现传播给了更广泛的读者。梅森的声名主要来自于他作为国际科学交流的中介人地位，通过他，数学家可以广泛地传播自己的思想。

39

如同数代人被搜寻素数规律所迷倒一样，梅森对此同样着迷。尽管他无法找到一个生成所有素数的公式，但是他发现了一个远比费马公式成功得多的公式。与费马一样，梅森同样考虑 2 的方幂，但是不像费马那样加上 1，梅森决定在结果中减去 1，结果 $2^3-1=8-1=7$ 为素数。也许梅森的音乐直觉对他有了帮助，倍增一个音的频率将会提高这个音八度，因此 2 的方幂产生和谐的音符。你也许可以想象得到，一度的偏移将会是一个与原始频率不谐调的音符，就是一个“素”音符。

梅森很快就发现，自己的公式并非每次都能产生素数，像 $2^4-1=15$ 就不是素数。梅森意识到，如果 n 不是素数的话，2^n-1 也不可能为素数。于是他大胆宣称，对 257 以下的 n，如果 n 为 2，3，5，7，13，19，31，67，127，257 中的某一个，那么 2^n-1 将会是素数。他还发现，即使 n 为素数，也仍然不能保证 2^n-1 为素数。他手工计算了 $2^{11}-1$ 得到 2047，这是 23×89。对于梅森断言如此大的 $2^{257}-1$ 为素数，数代数学家都认为是奇迹，要知道这个数有 77 位。是不是这个修道士有某个神秘的算法，告诉他这个超越任何人计算能力的数，是一个素数呢？

数学家相信，如果继续计算梅森数，那么将有无穷多个 n 可以保证梅森数 2^n-1 为素数，但是我们同样缺乏证明来保证这个猜想的正确性。我们仍然在等待一位现代的欧几里得来证明梅森数是无穷尽的，或者这个遥远的山峰只是数学上的幻象。



与费马和梅森同时代的许多数学家将素数的有趣计数性质作为娱乐，但是他们的方法根本不符合古希腊人证明的思想。这也部分地解释了为什么费马没有给出他宣称的结果的详细证明，在那个时代，人们明显缺乏给出逻辑解释的兴趣。数学家满足于该学科实验性的进展，在一个高速增长的机械化时代，结果只需要用实例来验证就可以了。然而在18世纪，出现了一位数学家，他重新复苏了数学中证明的价值。他就是生于1707年的瑞士数学家莱昂那德·欧拉（Leonhard Euler），欧拉解释了许多费马和梅森发现但是没有证明的规律。他采用的方法非常重要，为我们理解素数打开了一扇新的理论窗口。

欧拉，数学之鹰

18世纪中期是宫廷赞助（court patronage）时期。此时的欧洲正处于革命前夕，所有国家都在专制君主的统治之下：弗雷德里克大帝在柏林；彼得大帝和凯瑟琳女皇在圣彼得堡；路易十五和路易十六则在巴黎。在他们资助下的学术活动推动了知识分子启蒙运动的发展，实际上他们认为这样做，即宫廷中充满了知识分子的氛围，是一种身份的象征。同时他们也深知科学与数学的潜力所在，就是能推进本国的军事和工业能力。

欧拉是一位牧师的儿子，他的父亲希望自己的儿子能子承父业。然而，年轻的欧拉早早表现出来的数学天才使那些掌权者都注意到了他，不久所有欧洲的学术单位都竞相邀请欧拉加盟。他曾在当时的数学中心巴黎科学院待过一段时间，在1726年他决定接受邀请，加入圣彼得堡科学院，那是彼得大帝推动的俄罗斯教育改革运动的顶点。来自巴塞尔，曾经在童年时代激发起欧拉对数学的兴趣的朋友，从圣彼得堡写信给欧拉，让他从瑞士顺路带来十五磅咖啡、一磅顶级绿茶、六瓶白兰地、十二打上好烟斗以及数十副纸牌。受礼物的拖累，年轻的欧拉花了七个星期，利用水路、步行和邮车，终于在1727年5月来到圣彼得堡，

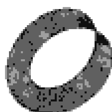


追寻自己的数学之梦。在随后的岁月中，欧拉做出了大量的成果，在1783年欧拉去世之后的50年里，圣彼得堡科学院仍在源源不断地发表那些库存材料。



图8　莱昂那德·欧拉（1707～1783）

欧拉在圣彼得堡时期的一个故事极好地说明了宫廷数学家的作用。有一次，凯瑟琳女皇招待著名的法国哲学家和无神论者丹尼斯·狄德罗（Denis Diderot）。狄德罗经常批评数学，认为数学对实践毫无帮助，好



像在人类与自然之间拉上了一层幕布。然而凯瑟琳女皇很快就对她的来宾感到厌倦，并不是因为狄德罗轻视数学的态度，而是因为他无休止地谈论她的国家的宗教信仰问题。此时欧拉被宣召到宫中帮忙，让这位令人厌倦的无神论者安静下来。为了感谢凯瑟琳的厚待，欧拉接受了这个任务。他在众人的面前严肃地对狄德罗说，“先生，$(a+b^n)/n=x$，因此上帝存在。请回答！”据说当时狄德罗就被这个数学命题吓退了。

42

这则趣事，是著名英国数学家奥古斯都·德·摩根（Augustus De Morgan）于1872年讲述的。也许其中会有一些添油加醋的地方，但是它反映了一个事实，就是大部分数学家都不太瞧得起哲学家。不过它确实表明了，如果没有数学家与天文学家、艺术家和作曲家一起，欧洲的皇家宫廷就不是完整的。

凯瑟琳女皇对上帝存在的数学证明并没有什么兴趣，但是她却对欧拉有关水力学、造船术与弹道学的工作有兴趣。这位瑞士数学家的兴趣涵盖了今天数学的很大一部分，除了用于军事的数学之外，欧拉还写了音乐理论。有趣的是，他的工作对音乐家而言太数学，对数学家而言又太音乐。

欧拉最为人熟知的故事是柯尼斯堡七桥问题的解答。现称为普雷高亚河（River Pregolya）的普雷盖尔河（River Pregel）流经当时普鲁士的城市柯尼斯堡（Königsberg，现在是俄罗斯的加里林格勒），在城市中心附近，普雷盖尔河中央分出了两个小岛，柯尼斯堡人在其上造了七座桥（参见插图9）。

曾经在市民中有这样一个挑战：是否有人可以绕行整个小镇，经过每一座桥一次并且只有一次，最后回到原来的出发点。欧拉于1753年最终证明了这个任务是不可能完成的，他的证明现在常作为拓扑学的入门内容。在拓扑学中，问题的实际物理维数常常是无关紧要的。起作用的是小镇各部分之间的连接网络，而非它们的位置或相对距离——伦敦的地铁示意图就可以很好地说明这一点。

在欧拉的心中，数是高于其他一切的。正如高斯所写的那样，



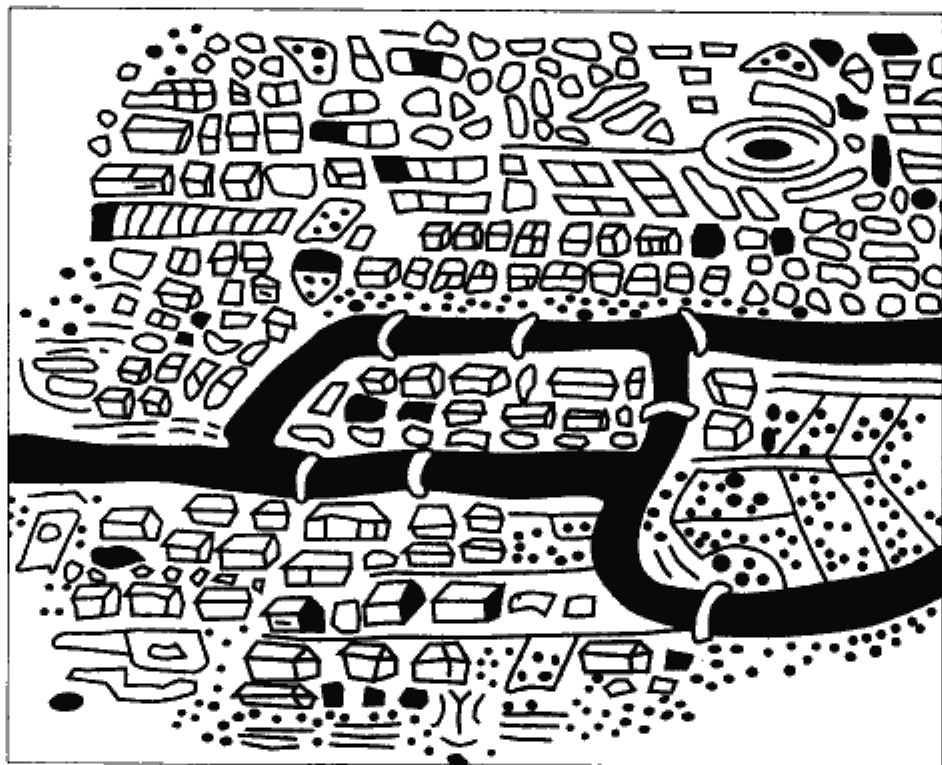
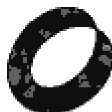


图 9　柯尼斯堡的七座桥

> "这个领域的特殊之美吸引了那些曾经活跃于该领域的人们，欧拉曾多次将它表达出来。欧拉在几乎每一篇有关数论的文章中，都频繁地提到他在探索中得到的欢乐，并且他的工作发生了受人欢迎的改变，变得与实际应用的联系更加直接。"

43

欧拉对数论的热情来自于与克里斯蒂安·哥德巴赫（Christian Goldbach）的通信。哥德巴赫是生活在莫斯科的一位业余德国数学家，担任圣彼得堡科学院的非正式秘书。像之前的业余数学家梅森一样，哥德巴赫同样着迷于数的游戏与数字实验。正是在与欧拉的通信中，他猜想每一个偶数都能写成两个素数的和。在给哥德巴赫的回信中，欧拉则寄给他许多自己找到的关于费马那些神秘发现的证明。相比较于费马将他的假想证



明作为一个秘密，欧拉更乐于向哥德巴赫炫耀自己证明了费马关于某些素数可以写成平方和形式的断言，甚至欧拉曾试图证出费马大定理的一个特例。

抛开对证明的热爱，欧拉本质上更多的是一位实验数学家。他的许多论证都跟随于当时数学界的风气，包含一些不严格的步骤。如果能找到一个有趣的新发现，这些不严格的步骤并不会影响欧拉。欧拉是一位拥有杰出计算能力的数学家，并且是一位操作数学公式的能手。正如法国院士佛朗索瓦·阿拉戈（François Arago）评价的那样，“看上去欧拉可以毫不费力地进行计算，如同人类呼吸，或是鹰在天空中翱翔那样自然。”

44

除此之外，欧拉很喜欢计算素数。他制作了包含 100 000 以内所有素数的素数表，甚至还包括了一些更大的素数。在 1732 年，欧拉首先证明了费马的素数公式 $2^{2^N}+1$ 在 $N=5$ 时失效：利用新的理论思想，他找到了如何将这个 10 位数分解为两个更小的数的乘积的方法。欧拉最不寻常的结果之一是他找到一个公式，看上去可以生成一部分素数。在 1772 年，他计算了将 0 到 39 分别代入公式 x^2+x+41 后得到的答案，如下表所示：

41，43，47，53，61，71，83，97，113，131，151，173，197，223，251，281，313，347，383，421，461，503，547，593，641，691，743，797，853，911，971，1033，1097，1163，1231，1301，1373，1447，1523，1601

欧拉感到很奇怪，为什么这个公式可以产生如此多的素数。但是他也知道这个过程将在某个点失效。也许你很清楚，当你将 41 代入公式，所得的结果肯定可以被 41 整除。同样在 $x=40$ 的时候，你也会得到一个非素数。

尽管如此，欧拉还是很震惊于这个公式生成素数的能力，他开始思考除了 41 之外是否还有别的数有这样的能力。他发现如果你取 $q=2$，



3，5，11，17，当你输入 0 至 $q-2$ 的数时，公式 x^2+x+q 都将生成素数。

但是找到一个像这样简单，并且能生成所有素数的公式，即使是伟大的欧拉也无法做到。他在 1751 年写道，“人类的思想永远也不能看透其中的某些神秘性，无奈我们只能看见素数表中的一小部分，我们相信其中的主宰既非有序也非规律。”我们构建了有序的数学世界于这些基本的物体之上，可是它们本身却是如此广泛而又不可预测，这难道是合理的吗？

事实证明，欧拉已经站在某个能破解素数僵局的公式的门外。然而欧拉无法解决的东西，仍然在等待另外一个百年，以及另外一个伟大的思想。这个思想属于伯纳德·黎曼（Bernhard Riemann）。不过仍然是高斯横向思维的结果，最终激发了黎曼的新思想。

45

高斯的猜想

如果经过数个世纪的努力，仍然无法找到某个能生成全部素数的公式，也许最好的办法就是采取新的策略。这也正是年仅 15 岁的高斯在 1792 年时的想法，此前一年他得到了一本有关对数的书籍作为礼物。数十年前，每个在学校中学习计算的年轻人都熟悉对数表，但由于口袋式计算器的出现，现今对数表已失去了往日的地位。不过在数百年前，每一位航海家、银行家和商人都需要利用对数表，将复杂的乘法转化为简单的加法。在高斯得到的书籍最后，附有一张素数表。在一本对数书中出现素数表，这是很奇怪的一件事。经过仔细的计算，高斯发现在这两种看上去毫不相干的事物之间似乎存在着某种联系。

第一张对数表出现于 1614 年，当时巫术与科学共存。对数的创造者，苏格兰男爵约翰·纳皮尔（Baron John Napier），被当地人认为是从事黑暗法术的魔法师：他身穿黑衣躲藏在他的城堡中，一只漆黑的公鸡立在他的肩头，嘀咕着他对于大灾难的代数预言，即最终审判将发生在



1688 年至 1700 年之中。不过他既将自己的数学才能应用在玄学上，同时也揭示了对数函数的魔力。

如果你在计算器上输入 100，然后按下“log”键，计算器就可以输出 2，这就是 100 的对数。你的计算器所做的工作就是：找出数 x 使得方程 $10^x = 100$ 成立，在此情况下计算器的输出值是 2。如果你输入 1000，它是 100 的十倍，计算器输出的结果将是 3，此时对数结果增加了 1。这就是对数的根本特征，它将乘法转化为加法。我们输入的数变为 10 倍时，只需在以前的结果上加 1 就可以了。

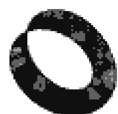
另一个重要的结果是，数学家发现可以研究那些并非 10 的整数幂次的数的对数。比如说，高斯肯定可以在对数表中查 128 的对数，并发现 10 的 2.10721 次方将很接近于 128。这些计算结果在 1614 年被纳皮尔搜集起来构成了他的对数表。

46

17 世纪是商业和航海业蓬勃发展的时期，对数表的出现更加速了这一进程。因为对数在乘法和加法之间搭起了一座桥梁，原先两个大数相乘的复杂工作就可以转化为简单的将两数的对数相加。为了求得两个数的乘积，商人先将原先两个数的对数相加，然后通过对数表反查出最后的结果。通过这些对数表获得的计算速度的提高，可以避免船只的失事或交易的失败。

不过在小高斯得到的对数书中，他最着迷的是最后附加的素数表。与对数表相比，这个素数表对于那些注重实际应用的数学家而言，并无任何重要之处。（安东尼奥·菲科尔（Antonio Felkel）在 1776 年编制的素数表被认为是无用之物，最后在奥地利与土耳其的战争中，竟被用来包裹子弹！）对数非常易于预测，可是素数则完全随机，人们完全无法预测 1000 之后的第一个素数出现在何处。

高斯采取的重要步骤就是问了一个全新的问题，而非试图去预测下一个素数的所在。他试着估计在 100 之内究竟有多少个素数，在 1000 之内有多少个素数，等等。如果任意给定一个数 N，是否存在某个方法，可以估计从 1 到 N 之间素数的个数？比如说，在 100 以内有 25 个



素数，也就是说如果你随机抽取一个在1至100之间的数，你得到素数的机会是四分之一。这个比例在1至1000之间，甚至是1至1 000 000之间又如何呢？利用拥有的素数表，高斯开始着手研究这个问题。通过审视素数的比例，高斯发现随着数的增加，某个规律也开始显现。抛开素数的随机性，一个令人惊讶的规律似乎逐渐从迷雾中显现了出来。

如果我们仔细观察一下下面这张基于现代计算的、包含10的不同幂次的素数个数表，就能看出这个规律。

这个表包含的信息比高斯发现的更多，并且清晰地显示出高斯发现的规律。这个规律清楚地表现在表中的最后一列。这一列表示了素数在所有数中占有的比例：当你数到100时，4个数中有一个是素数，因此要得到下一个素数，你平均要数的数字是4个；当你数到10 000 000时，15个数中有一个是素数。（因此在所有的七位电话号码中，大概有十五分之一的号码是素数。）在大于10 000的时候，最后一列的增幅大概是每次2.3。

47

N	1至N之间的素数个数，通常记为$\pi(N)$	平均经过几个数，你可以找到下一个素数
10	4	2.5
100	25	4.0
1 000	168	6.0
10 000	1 229	8.1
100 000	9 592	10.4
1 000 000	78 498	12.7
10 000 000	664 579	15.0
100 000 000	5 761 455	17.4
1 000 000 000	50 847 543	19.7
10 000 000 000	455 052 511	22.0

因此当高斯乘以10的时候，他就给所有数的个数与素数个数之比



值加上2.3，这个介于乘法与加法之间的联系，已经在对数中得到了很好的体现。利用手中的对数表，高斯立刻就发现他所面对的规律。

为什么每次高斯乘以10之后，这个比值增加2.3而不是1？这是因为素数喜爱的对数并非基于10的幂次，而是另外一个数。在计算器上输入100，然后按下“log”键，得到的结果是2，它是方程$10^x=100$的解。但这并不是说，我们只能使用10来进行计算，我们对自身10个手指的习惯才使得10如此重要。10所处的位置被称为对数的基底，我们讨论的对数，其基底可以为10以外的任何数。比如说，计算128相对于基底2的对数，就需要我们解决另外一个问题：找出x使得$2^x=128$。如果我们在计算器上有一个按键为“基底为2的对数”，我们就可以通过按这个键得到结果7，因为$2^7=128$。

48

高斯发现的素数的规律需要用到一个特殊数的对数，这就是e，它的十二位近似小数为2.718 281 828 459…（像π一样，它也是一个无限不循环小数）。e在数学中与π一样重要，并且出现在数学世界的每一个地方，这也就是为什么关于基底e的对数被称为“自然”对数的原因。

高斯在15岁时编制的表促使他得到下面这个猜想。对于1到N之间的数，大概每log（N）个数就会有一个素数。（此处log（N）表示N相对于基底e的对数）。因此他就可以估计在1至N之间，大概有N/log（N）个素数。高斯并没有宣称这是一个确切的有关N以内素数个数的公式——它仅仅是提供了一个很接近的估计。

高斯再次发现谷神星的时候应用了相似的原理。给定已有的观测数据，他的天文学方法可以很好地预测出天空中一个可供观察的小区域。对于素数高斯正是采用了同样的方法。多少年来，人们总是倾向于去预测下一个素数的准确位置，或是找到某个可以生成素数的公式。高斯并没有拘泥于一个数是否为素数这样的小事，通过退后一步并问了一个更普遍的问题：在100万之内有多少素数？而不是关注究竟哪些数是素数，从而找到了某种规律，一种逐渐显现的强烈的规律。



高斯对素数的考察还有着重要的心理学意义。高斯之前的人们在倾听素数的音乐时，注重的只是单个音符，因而无法听到整个作品；然而高斯考虑的是究竟存在多少个素数，因此他可以找到倾听主旋律的方法。

由高斯开始，大家习惯的将 1 至 N 之内的素数个数记为符号 $\pi(N)$。(此处 π 只是用于表示这个数，与圆周率 π 毫无关联。) 不幸被高斯误用的这个符号常常会导致人们联想到圆以及 3.1415…不过没关系，只要将它想成是计算器上的某个按钮就可以。当你输入某个数 N，并按下按钮 $\pi(N)$，计算器就会输出从 1 到 N 之间的素数的个数。因此 $\pi(100)=25$ 就是 100 以内的素数个数，同样的有 $\pi(1000)=168$。

值得注意的是，你可以用这个新的“素数个数”按钮，来准确地判断某个数是否为素数。当你输入 100 时，计算 1 至 100 之内的素数个数，你得到结果 25；如果你输入 101，结果变为 26，这就意味着 101 就是一个新素数。因此，只要 $\pi(N)$ 与 $\pi(N+1)$ 不一样，肯定就知道 $N+1$ 为素数。

49

为了清楚地表示高斯的发现有多奇妙，我们可以观察函数 $\pi(N)$ 的图像，图 10 就是当 N 为 1 至 100 时 $\pi(N)$ 的图像：

在这个小范围中，结果为跳跃的阶梯，因此很难预测下一级台阶出现在何处。同时在这样的范围中，我们还能看出素数的细节只是单独的音符。

下面让我们退后一步，在更大的范围中观察相同的函数。这次我们考虑的是 100 000 以内的素数（图 11）

此时单独的每一级阶梯已经变得无关紧要，我们最终看到的是这个函数逐渐形成的一个稍显拱形的曲线。这就是高斯听到的、可以用对数函数来模拟的主旋律。

素数如此不可预测，但其图像看上去却是如此光滑，这是数学中最神奇的发现，在素数的故事中标志着光辉的顶点。在其对数书的最后几页中，高斯记载了这个利用对数函数表示直到 N 的素数个数的公式。虽



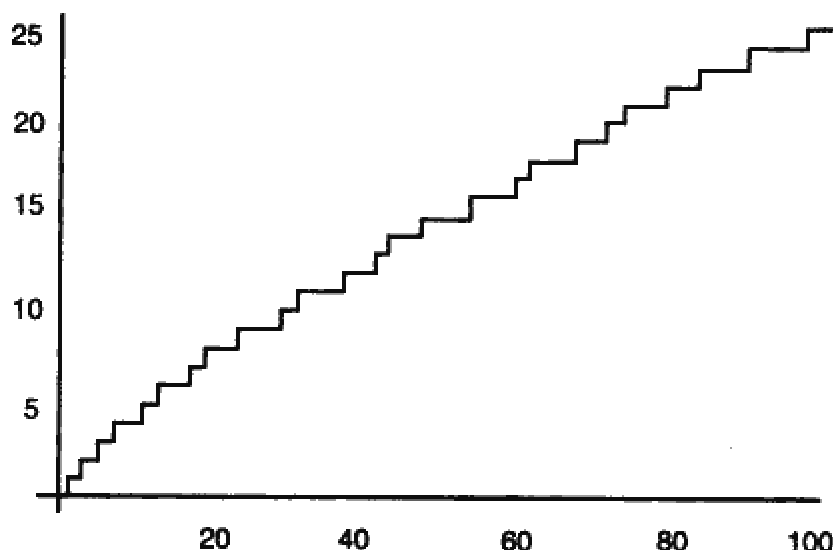


图 10　素数阶梯——100 之内的素数个数累积图

然这个发现很重要，但高斯并没有告诉其他人。数学世界对此发现的了解都隐藏在一些神秘词汇之下，"你永远无法知道，在对数表中可以发现多少诗意。"

50

为什么高斯对如此重大的发现抱以缄默，我们无法知晓。但事实是，高斯仅仅发现了素数与对数函数之间联系的证据，他知道自己绝对无法解释或者证明，为什么这两者之间会存在这样的联系。同样我们也无法知晓，这个规律是否会因为我们数的数越来越大而失效。高斯不愿意公开未证明的结论，标志着数学史上的一个重大转折。虽然古希腊人引入证明的思想是数学过程的一个重要组成部分，但是在高斯时代之前的数学家更关心的是数学上的科学猜测。如果数学可以应用到实际中，那么严格论证数学为什么可以有效地用于实际，则不是他们关心的问题，因此数学只是其他学科的工具。

高斯强调证明的价值，这就打破了当时的常规。对他而言，提供证明是数学家的首要目标，直到今天这仍然是基本准则。由于无法证明素



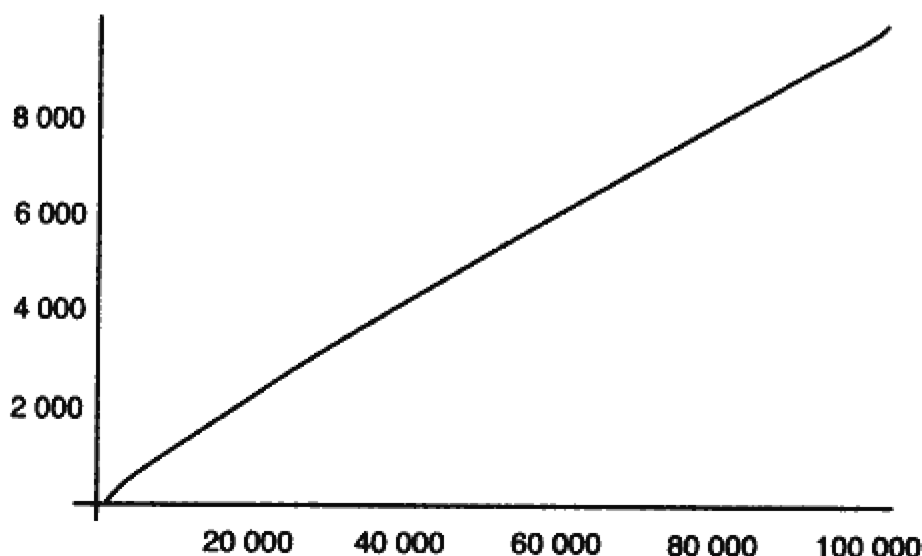


图 11　直到 100 000 的素数阶梯

51

数与对数之间的联系，高斯的发现对他而言就是无用的。不伦瑞克公爵提供的保护给了高斯相当大的自由，他可以挑剔地、甚至是任意地处理他做出的数学。他基本的动力不是名誉和赞誉，而是个人对其热爱的学科的理解。他的印章上刻着如下的座右铭：pauca sed matura（少而精）。一个结论除非已得到圆满解决，否则只能存在于日记或者对数表后面的涂鸦中。

对高斯而言，数学是一项个人的追求。他甚至用自己的秘密语言，将日记内容加密。但是有些日记却比较容易解读，比如说在 1796 年 7 月 10 日，高斯写下阿基米德的名言“找到啦!①”，后面跟着一个方程

$$\text{num} = \Delta + \Delta + \Delta$$

这表明他发现，每一个数可以写成三个数的和，这三个数来自于三角形

① Eureka，来自希腊数学家和发明家阿基米德发现测量不规则固体体积的方法，并以此发现测定金子纯度的方法时的惊呼。



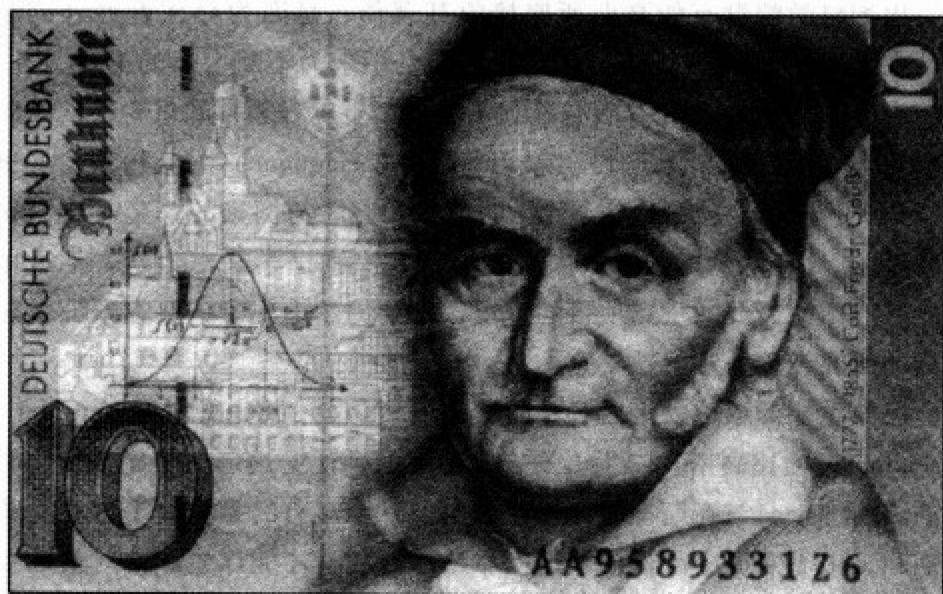


图 12　德国银行为纪念高斯而发行的十马克纸币

数 1，3，6，10，15，21，28……中，而三角形数曾被高斯在中学课堂中用来推导出自己的求和公式。举例而言，50 = 1 + 21 + 28。但是有很多日记仍然无法解读，是一个完完全全的谜题。高斯在 1796 年 10 月 11 日写下的“Vicimus GEGAN”，就没有人知道其含义。有人谴责高斯没有及时公布其发现，因而阻碍数学的发展至少半个世纪。如果高斯不是那么固执地追求每个发现的确切解释，或是没有将日记加密的话，数学也许能以更快的步伐前进。

52

有些人认为高斯之所以不公开那些结果的原因，是因为巴黎科学院曾因晦涩难懂拒绝过他有关数论的巨著《算术探讨》。在受到这样的打击之后，为了免于更多的耻辱，他坚持在完成数学上每一个必要步骤之前，决不公开出版任何发现。《算术探讨》没有得到人们的欢迎，部分原因也是因为高斯在面向大众的著作中同样进行了加密。他总是认为数学如同一幢建筑物，建筑师不可能留下脚手架，让人们知道如何去建造一幢高楼。这样的哲学使得数学家无法领悟高斯的数学。



巴黎科学院没有如高斯所愿接收其著作，是因为存在着另外的原因。在18世纪末期，巴黎的数学更多的是用来为不断增长的工业服务。1789年的法国大革命让拿破仑看到了加强军事工程教育的重要性，因此他投资建立了高等综合理工学院（École Polytechnique）为其将来的战争目标服务。拿破仑曾说过，“数学的进步和完善与国家的繁荣有着密切的联系。”因此法国的数学家大多专注于解决弹道学和水力学。不过抛开这些对国家需要的重点项目的重视，巴黎仍然出现了一些在欧洲首屈一指的研究纯粹数学的数学家。

巴黎重要的权威人士之一是阿德里安-马里·勒让德（Adrien-Marie Legendre），他比高斯大二十五岁。画像上的勒让德是一个略显自大、丰满的圆脸绅士。与高斯不同，勒让德生于一个富有的家庭。不过在大革命期间，由于家道中落，他被迫依靠自己的数学才能谋生。他对素数及数论同样感兴趣，在1798年（高斯给出近似公式后6年）他宣布了有关素数与对数之间的实验联系的新发现。

尽管最终的事实证明高斯在素数估计问题上击败了勒让德，但是当时勒让德确实对小于 N 的素数个数的估计做出了改进。高斯曾经粗略地估计小于 N 的素数个数为 $N/\log(N)$，但这只是一个比较接近的估计。后来发现当 N 变得越来越大时，这个估计离真实值的偏差也越来越大。在高斯早期猜想的对比图中，下面的线代表高斯的估计，上面的线代表真实的素数个数：（图13）

53

这幅图表明虽然高斯已经找到了某些东西，但事实上仍然有改进的空间。

勒让德的改进是将 $N/\log(N)$ 改写成

$$\frac{N}{\log(N)-1.08366}$$

这样引入的小小的改进，使得高斯的曲线向上移动，更加接近于真实的曲线。在当时的所能计算到的数值范围中，已经无法分辨图像 $\pi(N)$ 与勒让德的估计之间的差别了。由于完全沉浸在当时占据优势的应用数



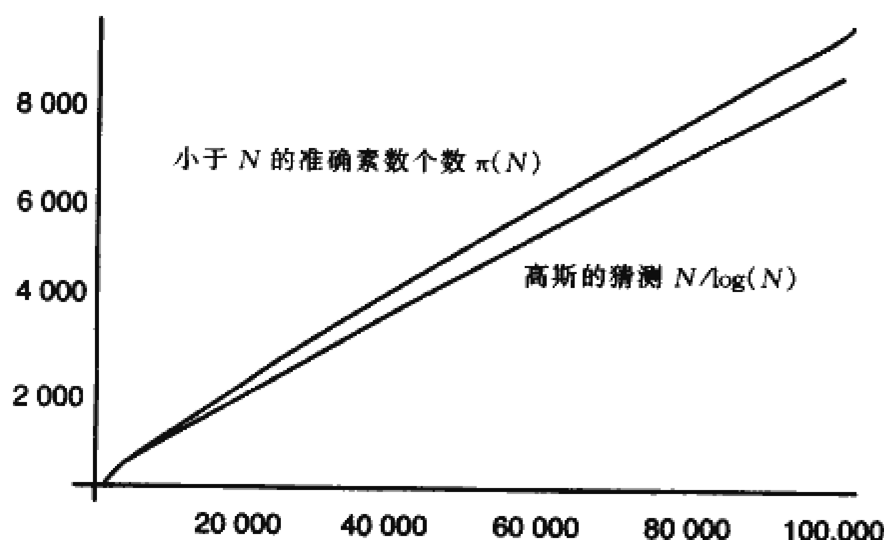


图 13 高斯的猜测与准确素数个数之间的对比

学问题之中，勒让德不太愿意抽空来做更多有关素数和对数之间联系的预言。不过勒让德并不害怕公开那些未证明的思想，或是有证明缺陷的结果。1808 年他在一本名为《数论》（*Théorie des Nombres*）的书中公布了他的猜想。

究竟谁首先发现素数与对数之间的关系，导致了勒让德与高斯之间一场激烈的论战。战火甚至弥漫到了素数之外，勒让德宣称，高斯用来预测谷神星轨道的方法也是他首先发现的。更多的是，当勒让德宣称他发现了某个数学结果时，伴随而来的则是高斯的公告，声称他早已经发现了这个结果。在 1806 年 7 月 30 日写给一位天文学同事舒马赫①的信中，高斯埋怨道，"我所有的理论工作都与勒让德的工作如此相似，也许这就是我的命运吧。"

54

① Heinrich Christian Schumacher，1780 ~ 1850，德国天文学家、曾担任曼海姆天文台台长和哥本哈根大学教授。



由于高斯生性骄傲，在他的一生中，他根本不愿牵涉进那些与权威的公开论战之中。高斯去世后，人们在检查其论文及通信时才发现，那些荣誉确实应该归于高斯。直到1849年，人们才知道在素数与对数的关系这个问题上，高斯击败了勒让德。这个关系出现在那年的圣诞夜他写给数学家及天文学家乔安·恩克（Johann Encke）的信中。

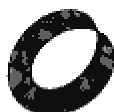
在19世纪初期的实际计算中，勒让德的函数用来估计小于N的素数个数，确实比高斯的公式要好。只是那个看上去相当粗糙的修正项1.08366，使得数学家相信肯定有着更好的、更自然的东西隐藏在背后，从而可以更好地掌握素数的行为。

这些粗糙的数，在其他学科中也许很常见，但是数学世界更青睐那些最优美的构造。我们将会看到，黎曼假设可以作为一个例证，来解释数学家持有的一种普遍的哲学思想：在粗糙世界与优美世界之间进行选择，大自然总是会选择后者。数学就该如此，这是令大部分数学家感到惊讶的原因所在，同样也可以解释为什么他们总是如此迷恋于这门学科的美。

因此我们不应该感到奇怪，高斯在后来的日子中将这个猜想作了进一步的优化，得到了一个更为准确的函数，并且更加优美。同样在那封圣诞夜写给恩克的信中，高斯解释了他是如何得到一个比勒让德的改进结果更好的估计的过程。高斯所做的就是回到他童年探索的出发点，他曾经计算过在前100个数中，有四分之一为素数；在前1000个数中，出现素数的几率下降到了六分之一。由此高斯认识到，你数的数越多，出现素数的几率就越小。

因此高斯的脑海中逐渐形成了一幅自然界究竟如何决定一个数是否为素数的画面。由于素数的分布看上去很随意，抛硬币未尝不是一种决定素数的好模型，正面朝上就是素数，背面朝上就不是素数。但大自然是否抛过硬币呢？此时高斯认为，这枚硬币可以被加权。加权的结果就是，它正面朝上的几率不再是二分之一，而是$1/\log(N)$。因此数1 000 000为素数的概率就是$1/\log(1\ 000\ 000)$，这大概是十五分之一。

55



因此当 N 越来越大时，N 为素数的几率也就越小，因为正面朝上的几率 $1/\log(N)$ 越来越小。

这只是一种试探性的过程，因为 1 000 000 和其他任意给定的数或者为素数，或者不是，这样的事实并不能由抛硬币改变。虽然高斯脑海中的模型对于预测某个数是否为素数没有任何用处，但是他发现这对于预测稍弱的问题，即可以碰到多少个素数的问题十分有用。他用这个模型来估计当你抛了“素数硬币” N 次之后，你得到的素数个数。如果使用普通硬币，正面朝上的概率为二分之一，因此有 $N/2$ 次是正面朝上。但是“素数硬币”正面朝上的概率随着每一次抛出越来越小，因此在高斯的模型中，素数的个数可以预测为

$$\frac{1}{\log(2)}+\frac{1}{\log(3)}+\cdots+\frac{1}{\log(N)}$$

实际上高斯更进一步地得到了一个被他称为是对数积分的函数，记为 $\mathrm{Li}(N)$。新函数是基于上述概率和的一个微小变形，结果十分精确。

在高斯 70 岁时，他写信给恩克，说自己已经建立了直至 3 000 000 的素数表，“我经常利用每小时中的一刻钟空闲时光来进行一千个数的计算”。高斯利用对数积分估计的小于 3 000 000 的素数个数仅仅和准确值相差万分之七。勒让德曾经对其粗糙的公式进行过修改，以与 $\pi(N)$ 相符，因此以当时的数据看来，勒让德的公式更加准确。但是随着更大范围素数表的建立，人们发现勒让德的公式对于超过 10 000 000 之后的素数个数根本谈不上精确。布拉格大学的教授雅库伯·库力克（Jakub Kulik）花了 20 年的时间，独力完成了 100 000 000 之内的素数表。这部完成于 1863 年的洋洋八卷巨著从没被出版，只是收藏于维也纳科学院的文献之中。虽然从第二卷开始数据已经开始错误，但是这份表格仍然说明高斯基于 $\mathrm{Li}(N)$ 函数的方法，远胜于勒让德的方法。现代的素数表则表明高斯的直觉是多么的准确，他对于 10^{16}（10 000 000 000 000 000）以内的素数个数估计值与真实值只相差了十亿分之一，而勒让德的公式则相差了千分之一。勒让德试图通过修改公式来模拟已知数据的方法，

56



被高斯的理论分析彻底击败。

高斯在自己的方法中注意到一个奇怪现象：在所知的 3 000 000 以内的素数范围中，公式 Li（N）总是过多地估计素数的个数，于是他猜测这个事实永远成立。现代的数值计算证据已证实高斯的猜想在 10^{16} 以内均成立，还有谁会怀疑高斯的直觉？在绝大多数实验室中，任何得到 10^{16} 次相同答案的试验已经可以被认为是绝对可信的结果了——但是数学家不会承认。不过这一次，高斯的直觉出了错。另一方面，虽然数学家最终证明了 π（N）会超过 Li（N），但是没有人可以见到其发生，因为我们永远也不可能数到那么大。

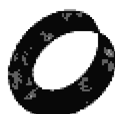
π（N）和 Li（N）的图像对比说明了这是一个十分好的拟合，在如此大的范围中，想要将两者区分几乎是不可能的。但要强调的是，如果在这幅图上的任一部分使用放大镜你就会发现这两个函数是完全不同的。π（N）的图像看上去是阶梯状的，而 Li（N）的图像则是光滑的、没有任何跳跃的图像。

高斯揭示了这样一个事实，即自然界通过抛硬币来决定素数。硬币被赋予不同的权重，使得一个数 N 有 log（N）分之一的机会成为素数。但是他仍然没有找到一种方法，来准确预测每一次抛硬币的结果。这一点仍需要新一代数学家的洞察力。

利用转换观察问题的方式，高斯察觉到了素数中的规律，这个猜想后来被称为素数猜想。要证实高斯的这个猜想，数学家需要证明，高斯的对数积分和真实素数个数之间的百分误差会越来越小。高斯看见了这座遥远的山峰，从而留给后代一项工作，就是提供一个证明，来揭示那条通往高峰的道路，或是揭去那幻象的面纱。

人们埋怨谷神星的出现，转移了高斯对证明素数猜想的注意力。高斯在 24 岁时突然得到的名声促使他转向天文学，从此数学在他心中不再占有首要的地位。在 1806 年，高斯的资助人费尔南德公爵被拿破仑杀死，他不得不寻找工作以供养家庭。高斯拒绝了圣彼得堡科学院提供的、接替欧拉职位的建议，而是接受了撒克逊地区一个小的大学城哥廷

57



根天文台台长的职务。高斯花费了很多时间在夜间寻找更多的小行星，并完成汉诺威和丹麦政府委托的关于国土的测量工作，但是他仍经常思考数学问题。在他标注汉诺威的山脉时，他会考虑欧几里得的平行线公理；回到天文台之后，他又会接着扩充他的素数表。高斯是最先听到素数音乐主旋律的人，而作为他为数不多的学生之一，黎曼发现了那隐藏在素数杂音背后的旋律，并将其能量完全释放了出来。 58

第三章

黎曼的数学照虚镜

难道你没有感觉到它，听到它吗？难道只有我一个人听到这奇妙的、轻柔的旋律吗？

——理查德·瓦格纳（Richard Wagner）

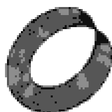
《特里斯坦与伊索尔特》第三幕第三场

1809年威尔海姆·冯·洪堡（Wilhelm von Humboldt）成为普鲁士王国北德国地区的教育部长。在1816年给歌德的一封信中，他写道，“我在这里忙于大堆的科学事物，但我也深深地感受到强大的旧习俗影响着我，而新事物又令我厌恶……”洪堡推进的一项运动，是将科学从作为工具的境地中解放出来，重新回归古典传统的对知识本身的追求中。此前制定的教育计划都是为普鲁士的荣耀提供所需的技术人员。不过从此以后，教育则更重视个体发展的需要，而非国家的需要。

作为一个思想家和政府官员，洪堡发起了一场具有深远意义的变革。被称为高级中学（Gymnasium）的新学校在普鲁士全境及附近的汉诺威地区纷纷建立，这些学校的教师都不是来自旧教育系统的教士成员，而是那些当时新建立的大学和理工学院的毕业生。

洪堡称之为“现代大学之父”、成立于1810年法国占领时期的柏林大学则是皇冠上的珍珠。柏林大学座落于椴树下大街[1]，前身为普鲁士

① The grand boulevard Unter den Linden，也称为菩提树下大街，位于德国柏林，是欧洲最著名的大街之一，是柏林市中心的交通枢纽，并且将众多的景观和名胜连接在了一起。



王子海因里希的王宫。柏林大学是最先倡导科研与教学并进的学校。“通过大学的教育不仅能够理解科学的整体性，更重要的是能促进科学的发展”，洪堡说。抛开他对古代世界的热情，柏林大学在洪堡的指导之下，除了经典的法律、医学、哲学和神学之外，在引进新学科方面同样走在了前面。

因此，数学首次成为了高级中学和大学教程中的一个重要组成部分。鼓励学生学习作为独立学科，而不是简单地为其他学科服务的数学，这与拿破仑死板的教育改革形成了鲜明的对比。在拿破仑统治的法国，数学只是用来加强法国军事目标的工具。法国数学家约瑟夫·傅里叶（Joseph Fourier）曾批评德国学校的教育忽视了那些实际问题，柏林大学的教授卡尔·雅各比（Carl Jacobi）在1830年写给巴黎的勒让德的信中，对这件事做出如下回应：

> 傅里叶先生认为数学的主要目的是公众的应用和解释自然现象，这是没错的。但是像他那样的哲学家也应该知道，科学的唯一目标是人类心智的荣耀。在这种观点之下，数论之中的问题与世界系统的问题应该是具有相同价值的。

对拿破仑而言，只有教育可以最终摧毁大革命之前的社会与政治制度。他认为教育就是建立新法国的支柱，因此当时于巴黎建立的数所高等院校直到今天仍然声名显赫。不仅是学校的领导阶层允许来自各种背景的学生入学，而且教育更重视那些服务于社会的科学。在法国大革命中，某地区的官员在1794年写信给某位数学教授，自荐教授一门“共和算术”的课程：“市民们，大革命不仅提升了我们的道德水准，为我们及我们的后代铺平了通往快乐的道路，它也粉碎了那些阻碍科学前进的枷锁。”

与这种穿越边界流传而来的功利主义哲学相比，洪堡关于数学的计划就完全不同。德国教育革命的效果对数学家理解这门学科的许多方面有着深远的影响。数学家可以建立新的、更加抽象的数学语言，特别是

对素数的研究也将产生新的革命。

曾经繁荣的商业中心、汉诺威的小镇吕内堡（Lüneberg）也受到了洪堡改革的影响。持续了数世纪的商业嘈杂声已不再出现在那些鹅卵石小道上，取而代之的是1829年新建的一幢建筑物，它矗立在哥特教堂三座尖塔的中间，这就是约翰纽姆高级中学(The Gymnasium Johanneum)。

到了19世纪40年代初期，这所学校已经很繁荣。校长舒马福斯（Schmalfuss）是洪堡提出的新人文主义思想的热情支持者。他的图书馆完美地表现了这一点：其中不光有德国经典与现代作品，还有从远方带来的书籍。特别的，舒马福斯尽量去获得那些从巴黎流传出来的书籍，因为在19世纪上半叶，巴黎是欧洲科学活动的中心。

60

在约翰纽姆高级中学，舒马福斯接受了一名叫作伯纳德·黎曼的学生。黎曼很害羞，不善于交朋友。黎曼原先在汉诺威另外一个小镇上中学，那样他可以和他祖母生活在一起。不过在他的祖母于1842年去世之后，黎曼被迫搬到吕内堡与一位老师生活在一起。在同班同学已经熟悉之后再加入这个集体，黎曼的生活并不开心。他开始思乡，并被同学嘲笑。有时他宁愿徒步走回他父亲在Quickborn的小屋，也不愿意和同龄人一起玩耍。

黎曼的父亲是Quickborn的牧师，他对自己的儿子抱有很高的期望。虽然黎曼在学校中并不开心，但他仍然勤奋和尽责地学习，不让自己的父亲失望。但是他不得不与自己的完美主义性格交战，对此老师也很头疼，因为黎曼经常不能按时交作业。对黎曼而言，除非答案是完美的，否则得不到满分将是一件不光彩的事情。他的老师因此怀疑他是否能够通过期末考试。

正是舒马福斯看到了这一点，并找到了让这个孩子的完美主义得到发展的方法。刚开始的时候，舒马福斯察觉到黎曼的特殊数学才能，并希望能促进这种能力的发展，于是他允许黎曼使用自己的图书馆。图书馆中有着丰富的数学藏书，在那里这个孩子就能摆脱与同学交往带来的社交压力。图书馆为黎曼开启了一个全新的世界，带来家一般的感觉，



并且他能掌握这一切。于是他进入了一个完美的、理想的数学世界，在这里，证明可以防止这个新世界的倒塌，数字成为了他的朋友。

将作为实践工具的科学教育转化为更加具有美学意义的对知识的追求，洪堡的倡议在舒马福斯的课堂上得到了很好的贯彻。舒马福斯指引着黎曼的阅读方向，让他从充满数学公式和定律的、为工业增长需求服务的数学教科书中解脱出来，接触欧几里得、阿基米德、阿波罗尼乌斯（Apollonius）等人的经典著作。正是有了这些人的几何学，古希腊人才理解了抽象的点和线，不再拘泥于几何学中特殊的公式。当后来舒马福斯给了黎曼更加现代的、由笛卡儿撰写的关于分析几何（充满了方程与公式）的巨著时，舒马福斯发现这本书中介绍的方法已经不能满足黎曼日益增长的对抽象数学的需求了。舒马福斯后来在一封给朋友的信中回忆道，"在当时他就已经可以说是一位数学家了，站在他的身旁，作为老师的我感到自己知识的贫乏。"

61

在舒马福斯的书架上有一本书，是他刚从法国得到的一本新书。这是勒让德出版于1808年的《数论》。在这本书中首次记录了在素数个数函数与对数函数之间存在的某种奇妙联系的观测结果。这个高斯和勒让德发现的联系仅仅是基于试验数据，当时还不清楚，当数字越来越大时，素数个数是否仍然可以用高斯或勒让德的函数来近似估计。

虽然这本四开巨著有859页之多，黎曼仍然迫不及待地读完了它。六天后，他将这本书还给了老师，"这本书很妙，我已经将它熟记在心。"当时舒马福斯几乎不敢相信。在两年之后的毕业考试中，他考了黎曼其中的内容，结果黎曼的成绩非常好。这标志着现代数学的巨人已经开始了他的数学生涯。多亏了勒让德，年轻的黎曼心中已经种下了一颗种子，在未来的日子中将会绽放出绚丽的花朵。

结束了毕业考试，黎曼渴望能进入那些促进教育革命的、充满活力的德国大学，不过他的父亲另有安排。由于黎曼的家庭很穷，父亲希望黎曼能像他一样进入教会工作，用牧师的工作为家庭带来稳定的收入，以抚养年幼的妹妹。汉诺威王国唯一设有神学课程的大学不是那些新成



立的大学，而是建立于1734年，大概一个世纪之前的哥廷根大学。遵从了父亲的意见，黎曼于1846年踏上了前往潮湿小镇哥廷根的道路。

哥廷根坐落于下萨克森地区的丘陵地带，是一座被城墙环绕的中世纪小镇。这个黎曼将要接触的地方，还保留着许多原先的特点，道路紧密地环绕着半木质的红瓦小屋。格林兄弟在哥廷根写了许多的童话故事，你甚至可以想象汉赛尔和格莱特兄妹①二人跑过镇里的小路。小镇中心是中世纪的镇议会大厅，墙上刻着“哥廷根之外没有生活”。这也正是大学中的人所体会到的感觉，因为学院生活完全是自给自足。在这所大学的早期，神学占有优势地位，但是从德国传来的学术风气也激发了哥廷根的科学气氛。在1807年高斯被任命为天文学教授以及天文台台长之后，哥廷根的声名随着科学而不是神学逐渐传开。

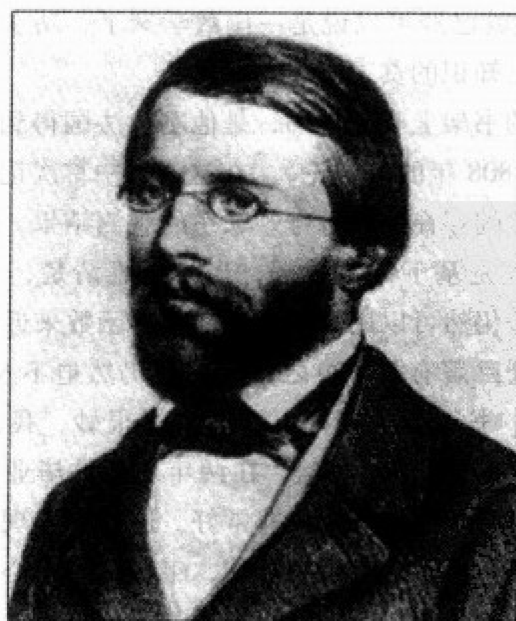


图14　伯纳德·黎曼，1826～1866

---

① *Hansel and Gretel*，格林童话中的一篇，讲述汉赛尔和格莱特兄妹被后母赶出家门后在森林的奇遇记。



此时，在年轻的黎曼心中，仍然燃烧着舒马福斯点燃的数学之火。他因为父亲的愿望来到哥廷根学习神学，但是伟大的高斯以及哥廷根的科学传统在第一年深深地影响了黎曼，因此希腊语与拉丁语的课程让位于物理与数学只是时间问题。由于父亲的赞同至关重要，黎曼小心翼翼地给父亲写了一封信，提出了想从神学转到数学专业的想法。不久他收到了父亲的祝福，感到如释重负，于是立即投入到大学的科学学习中去。

对拥有如此天赋的年轻人而言，哥廷根很快就不能满足他。不到一年的时间，黎曼已经用完了那些可用的资源。当时年老的高斯，已经基本上退出了大学里的学术生活——从1828年开始他每周只有一夜不在天文台。高斯在大学里仅讲授一门天文学课程，内容就是多年前令他声名鹊起的、重新发现“丢失的”谷神星的方法。黎曼不得不往别处寻找新的资源，以便能够激发他在学术上更进一步。不久他发现柏林是当时学术活动最活跃的地方。

柏林大学曾经受到过拿破仑建立的那些大学，像高等综合理工学院的极大影响，毕竟它是在法国占领时期建立的。当时主要的数学代表人物是彼得·古斯塔夫·勒让·狄利克雷（Peter Gustav Lejeune-Dirichlet）。狄利克雷是法国人，但他1805年出生在德国，1822年他回到巴黎寻根，在那里呆了5年，参与了不少学术活动。洪堡的兄弟亚历山大，一个业余科学家，在去法国的时候碰到了狄利克雷，对他留下了深刻的印象。于是他劝狄利克雷回德国，并且可以为他提供一个职位。也许是受到蔓延于巴黎街道的气氛的影响，狄利克雷的性格有些叛逆。在柏林，他经常开心地忽略那些大学权威所坚持的陈旧传统规定，并且用自己掌握的拉丁语来嘲笑这些规定。

哥廷根和柏林为像黎曼这样的科学界新人提供了两种截然不同的学术气氛。哥廷根大学沉浸于自身的独立与与世隔离，每个学期几乎没有外来学者进行学术交流，它是自给自足型的大学，它发达的科学来自于自身提供的动力。而柏林大学则因那些来自德国之外的交流而兴旺，来自法国的思想与德国人研究的自然科学结合在一起，产生了令人陶醉的



新式鸡尾酒。

哥廷根与柏林的不同氛围恰好对应于不同的数学家。有些人只有接触到外来的新思想才能成功，而另外一些人则因与世隔离而迫使自身找到新的力量和解释思想的新语言。黎曼需要与新思想接触，来取得学术上的突破，因此他知道柏林就是他要去的地方。

黎曼于 1847 年动身去柏林，并在那里待了两年。在那里，他得到了高斯早年的许多文章，在哥廷根，黎曼并没有能从沉默寡言的大师那里得到这些文章。黎曼还参加了狄利克雷的课程，后来在黎曼戏剧性的发现素数规律的故事中，狄利克雷也扮演了重要角色。从各方面来讲，狄利克雷都是一个能激发学生活力的教师。曾经参加过狄利克雷课程的一位数学家这样写道：

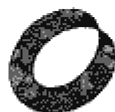
64

> 狄利克雷拥有丰富的知识和优秀的洞察力……他坐在高高的讲台上，面朝我们，眼镜推上额头，双手托着头……在他的手中仿佛有着虚幻的计算步骤，他将这些步骤念给我们听——我们好像也看到了这个过程，并理解了它们。我真是喜欢这样的讲课方法。

黎曼很快就与狄利克雷班上的几位年轻人交上了朋友，他们对数学也有着同样的热情。

此时在柏林还有另外的力量在产生。1848 年推翻法国君主制度的革命，从巴黎的街道迅速弥漫到了大部分欧洲，黎曼所在的柏林同样不能幸免。根据当时的记载，这件事对黎曼产生了很大的影响。有为数不多的几次，他与周围不同知识阶层的人走到了一起。同时他还参加了学生联合会，在柏林皇宫外面保卫国王，他还因连续 16 小时坚守岗位而声名远扬。

不过黎曼对于从巴黎流传出来的数学革命则持有另一种态度。当时的柏林不光从巴黎引进政治宣传材料，同时还引进不少著名的杂志和出版物。在收到了当时很有影响力的法国杂志《法国科学院院报》（*Comptes Rendus*）的最新一期之后，黎曼就躲进自己的小屋中，开始钻



研数学革命家奥古斯丁-路易斯·柯西（Augustin-Louis Cauchy）的论文。

柯西是大革命时代的孩子，他于1789年攻占巴士底狱前数周出生，当时生活物资的匮乏造成他营养不良。因此虚弱的柯西更愿意锻炼自己的思想，而不是强壮的体魄。遵循古老的传统，数学世界为柯西提供了一个避难所。柯西父亲的一位数学家朋友，约瑟夫-路易斯·拉格朗日（Joseph-Louis Lagrange），注意到这个年轻人的才能，对其他人评论道，"你看到那个小孩了吗？嗯，他将取代我们这些数学家。"但是他给柯西的父亲一个有趣的建议，"在17岁之前不要让他接触数学课本。"取而代之的是提高这个孩子的文学水平，以便最终在他回到数学世界之后，能有自己的数学语言，而不是从当时教科书中学来的语言。

65

事实证明这是一个合理的建议。在柯西与外部世界之间的闸门被打开之后，他培养出来的新语言就如洪水般一发不可收拾。柯西作品是如此之长，以致于《法国科学院院报》不得不强制执行对论文页数的限制，这个限制一直延续到今天。柯西的新数学语言对于同时代的人而言，实在是太先进，挪威数学家尼尔斯·亨力克·阿贝尔（Niels Henrik Abel）在1826年写道，"柯西是一个疯子……他所做的结果很好，就是很杂乱。最初我一点都不了解，现在我总算清楚一些了。"阿贝尔继续观察那些在巴黎的数学家，柯西是唯一一个研究"纯数学"的，而其他人"忙于研究磁学以及其他物理项目……他是唯一清楚该如何做数学的人"。

因为没有指导学生进行实际应用数学的研究，柯西与巴黎的权威产生了矛盾。他在高等综合理工学院执教的时候，当时的院长写信给他，批评他对于抽象数学过于着迷，"许多人认为，纯数学的指导在学院里已经够多了，并且未经允许的过度讲授会引起其他学科的不满。"因此年轻的黎曼着迷于柯西的工作也就不足为奇了。

由于黎曼对这些新思想是如此的着迷，有一段时间他几乎成了隐居者。在黎曼沉迷于柯西的结果时，他的同事根本就见不到他。数周之后，黎曼再次出现，并且断言"这是一门全新的数学"。紧紧抓住了柯



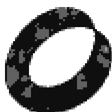
西和黎曼想像力的东西，正是刚出现的虚数的魔力。

虚数——新的数学风景

构建虚数的基本单位，是负一的平方根。这看上去似乎是一个矛盾，有人说允许这样的数就是将数学与其他学科割裂开来。要想接触这个数学世界，你必须拥有创造性的思想。初看上去，虚数与真实物理世界没有任何联系，物理世界看上去都是由那些平方为正数的数构成。然而，虚数不仅仅是一个抽象游戏，在20世纪的亚原子粒子世界中，它们起着决定性的作用。从大的范围来看，如果工程师们没有到过虚数的世界，飞机也不可能在天空中翱翔。那些只承认普通数的人永远也无法进入这个新世界。

如何发现这些新的数，起源于解方程的故事。古代巴比伦人和埃及人就已经认识到，如果要让3个人分7条鱼的话，像1/2，1/3，2/3，1/4这样的分数必然会出现在方程中。公元前6世纪，希腊人在研究三角形时发现，有时候用分数也无法表达三角形的边长，毕达哥拉斯定理（我国称为勾股定理）迫使他们发明那些无法用简单分数表示的新的数。比如说，取一个直角三角形，两条短边分别为单位长度，由毕达哥拉斯的著名定理可知，长边的长为方程 $x^2=1^2+1^2=2$ 的根，即边长为2的平方根。

分数在写成十进制展开的时候会出现循环规律，像1/7＝0.142857142857…，1/4＝0.250000000…。与它们不同，古希腊人证明了2的平方根不是一个分数，并且无论你计算到小数点后多少位，2的平方根的十进制展开都不会循环，其开头的几位如下：1.414213562…在哥廷根时，黎曼曾浪费了不少时间用于计算这些展开，他的纪录是小数点后38位。在没有计算器的情况下这是相当不错的成绩，但这也说明了哥廷根无聊的夜生活和黎曼本身不善交往的性格，他只能以这种方式作为晚间的娱乐。但是不管计算到多少位，黎曼清楚地知道他不可能



写下全部的展开，或者找到某种循环规律。

这些数除了表示为某些方程，像 $x^2=2$ 的根之外，几乎不可能用其他方式表达，由此特性数学家将之命名为无理数。这个名字反映了数学家对于无法精确写下这些数的某种无奈。但是，这些数确实有某种程度的存在性，它们可以作为一个点在直尺，或是数学家所称的数轴上表现出来。比如说，2 的平方根，大约是在 1.4 到 1.5 之间的一个点，如果你可以作一个标准的直角三角形，两个直角边长为 1，那么将斜边取出放在直尺旁边，你就能够确定那个代表 2 的平方根的点。

负数的出现，同样产生于解像 $x+3=1$ 这样的方程中。印度数学家在公元 7 世纪首先提出这些新的数。负数的产生是随着金融世界的发展而产生的，因为它们可以用来描述负债的状况。欧洲数学家花了 1 千年才接受了这个他们认为的“虚构的数”。负数在数轴上的位置位于 0 的左方。

67

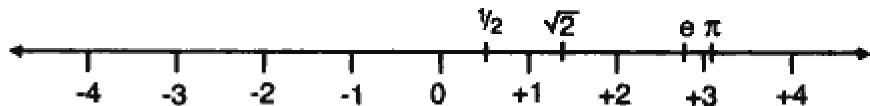


图 15　实数——每一个分数、负数或无理数均可以用数轴上的一个点来表示。

由于无理数和负数的出现，我们可以求解不同的方程。对于费马的方程 $x^3+y^3=z^3$，如果你不像费马当年那样坚持 x，y，z 必须为整数的话，我们可以找到一些有趣的结果。比如说取 $x=y=1$，z 为 2 的立方根，这个方程就可以成立。尽管如此，仍然有方程无法用这些已知的数轴上的数来求解。

对于方程 $x^2=-1$ 而言，好像没有一个数能成为它的解。毕竟无论是正数还是负数，它们的平方肯定是一个正数，因此满足这个方程的数肯定不是一个普通数。既然古希腊人在无法将 2 的平方根写为分数的时候，创造了一种新的数，为什么数学家不可以进行同样的想象，创造一个新的数来满足这个方程呢？这样的一种想像力的飞跃，对于任何学习



数学的人都是概念上的挑战。这个新的数，也就是负一的平方根，被称为虚数，记为符号 i。作为对比，数学家指出这样的数也像实数一样可以在数轴上找到。

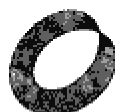
创造方程的解，看上去是无中生有，又像是在做假。为什么不接受一个方程无解这样的结论呢？这是一种很好的前进方式，但是数学家更加乐观，一旦我们接受了这个新数确实能够解原来的方程这个想法，这种思想上的飞跃带来的好处就远远强过任何起初的无奈。一旦被命名，它的存在就是不可避免的，它再也不是一个人工创造出来的数，而是一个一直存在的数，只是在我们提出正确的方程之前没有出现而已。18 世纪的数学家很勉强地承认，也许存在着这样的数。而 19 世纪的数学家已经足够勇敢地相信这种新的思想模式，并且向那些数学中已经接受的思想提出挑战。

68

老实说，-1 的平方根与 2 的平方根作为概念而言同样抽象，它们都可以定义为方程的解。但数学家是否需要为所有方程的解都定义新的数，比如说 $x^4=-1$？是否我们需要越来越多的符号表示这些解呢？正是高斯最终解决了这个问题，在他 1799 年的博士论文中，他证明了不需要再定义任何新的数，利用这个新发明的 i，数学家就能解决他们碰到的所有方程。每个方程的解都是由某些实数（分数和无理数）以及 i 的组合构成。

我们已经知道普通的数都位于数轴之上，数轴是一条从左至右的直线，其上的每一个点代表一个实数，这是自古希腊以来数学家早已熟知的事实。但是在这条数轴上已经没有空间留给虚数了，因此高斯证明的关键就是将这幅图进行扩展。如果你考虑另外一个方向会出现什么结果？用朝上的单位线段来表示 i 又如何？解方程需要的新的数，都是由 i 和普通数组合而成，比方说 $1+2i$，高斯意识到在这个二维的图像上，恰好有一个点对应着一个可能的数，数 $1+2i$ 就是先往右移一个单位，再向上移两个单位而到达的那个点。

高斯将这些数解释为虚数世界中的方向的集合。如果要将两个虚数



$A+Bi$ 与 $C+Di$ 相加，那么只需要按照两个点代表的方向，顺序移动过去即可。如果要将 $6+3i$ 和 $1+2i$ 相加，所得的结果就是 $7+5i$。（参见图 16）

尽管这是一个非常有效的辅助图形，但是高斯将这幅虚数世界的图像隐藏了起来。一旦他得到了自己的证明，这些辅助的图像就被去掉，以免留下痕迹。他很清楚在那个时代，人们对数学中的图像还存在着怀疑。在高斯年轻时的法国数学传统中，利用公式和方程的数学道路是占绝对优势的，因为这与当时的实用主义路线相吻合。当然，还有其他一些反对使用图形的原因。

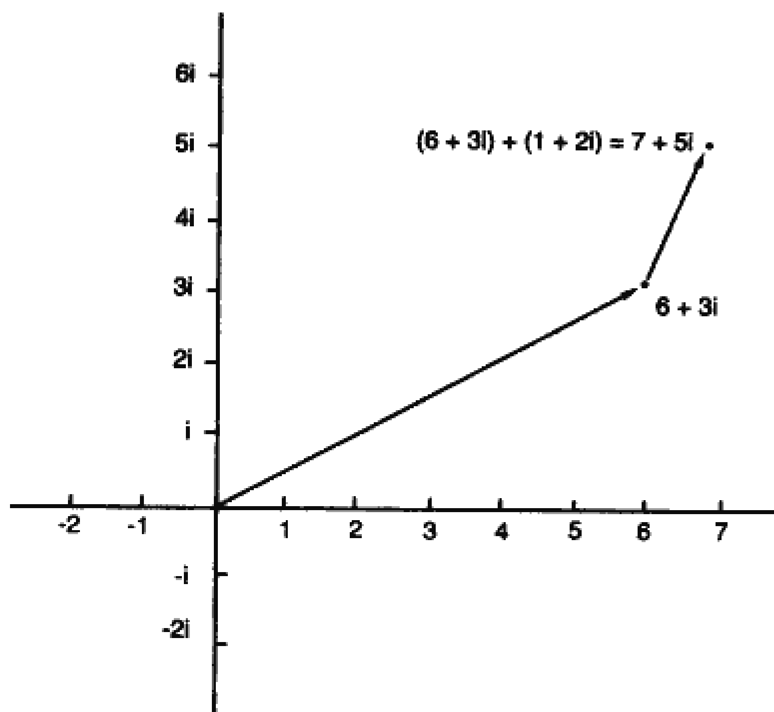


图 16　如何将两个虚数相加

数百年来，数学家认为图形具有误导的能力，毕竟数学语言的引入是为了描述物理世界。在 17 世纪，笛卡儿曾试图将几何学的研究转为



关于数和方程的纯论述，他的格言是"感觉即欺骗（Sense perceptions are sense deceptions）"。当黎曼在舒马福斯的图书馆里读到笛卡儿的著作时，他很不喜欢笛卡儿对物理图景的这种拒绝。

18 世纪末 19 世纪初期的数学家曾经被一个错误的图形证明所伤害。这是一个有关几何体的顶点数、边数和面数的关系公式，欧拉曾经猜想如果一个几何体有 C 个顶点，E 条边，F 个面，那么 C，E，F 满足关系式 $C-E+F=2$。比如说，一个立方体有 8 个顶点、12 条边和 6 个面。年轻的柯西在 1811 年基于图形直觉给出一个证明，但是后来却意外地发现了一个不满足这个公式的几何体——中心有洞的立方体。

70

柯西的"证明"漏掉了几何体可能存在洞的情况，因此需要在公式中再加上一项，来描述几何体存在洞的情况。由于图像可能掩盖了那些起初并不显现的部分，受此影响，柯西开始寻求公式所能带来的安全性。其中一个革命性结果就是他创造了一种新的数学语言，利用它数学家可以严格地讨论对称的概念，而无须借助任何图像。

高斯知道，在 18 世纪末期，他关于虚数世界的秘密图像可能会招致非议，因此他在证明中将其省略。数是用来相加与相乘的，而不是作出它们的图像。在大约 40 年之后，高斯终于承认他曾在论文中使用过那些图形。

镜中世界

即使没有高斯的图像，柯西与其他数学家仍然会开始研究，如果将函数的概念推广到这个新的虚数世界，而不是原先的实数世界时，究竟会发生什么事情。令他们吃惊的是，虚数为数学世界中看上去毫无关联的部分建立了新的联系。

一个函数如同一段计算机程序，在你输入一个数并进行计算之后，输出另外一个数。函数可以用某些如 x^2+1 这样简单的方程定义，当你输入 2 时，函数计算 2^2+1，结果输出 5。当然也存在着更加复杂的函



数。高斯感兴趣的是有关素数个数的函数，每次你输入一个数 x，函数就告诉你到 x 为止一共有多少个素数。高斯将这个函数记为 $\pi(x)$，这个函数的图像类似于上升的台阶，如第 50 页[①]的图 10 所示。每当你碰到一个素数，台阶就向上一格。当 x 从 4.9 增长到 5.1 时，素数个数就由 2 增加为 3，以记住新产生的素数 5。

不久数学家就意识到这些函数，像我们熟悉的 x^2+1，同样可以像普通数一样输入虚数值。如果我们将 $x=2i$ 代入函数，我们可以得到 $(2i)^2+1=-4+1=-3$。将虚数代入函数这个做法是从欧拉时代开始的，早在 1748 年，欧拉就在无意中发现了，如果利用这个镜中世界，本来毫无关系的数学分支将出现奇怪的联系。欧拉知道给指数函数 2^x 赋予普通数时，它的图像是急速上升的曲线。但是当他为这个函数赋予虚数时，他得到的是意料之外的结果：不再是指数上升的图像，而是波浪形的图像，就像我们熟悉的声波一样。产生这个图像的函数是正弦函数，正弦函数的图像类似于重复的波，每隔 360°，就能见到同样的图像。在每天大量的计算中都会碰到正弦函数，比如说，通过在地面测量角度的大小，可以用来计算一幢建筑物的高度。同样是欧拉那一代人发现正弦函数也是再现音乐的关键，我们用来调音的音叉发出的纯音 A 就可以用这样的波来表示。

71

欧拉将虚数代入函数 2^x，令他惊讶的是，产生的波函数对应于某个特定的音符。欧拉断定每个音符的特性是由对应虚数的坐标决定的。如果坐标越偏北，那么这个音越高；如果坐标越偏东，那么音量越大。欧拉的发现是最初的暗示，这些虚数将在数学世界中开启一条前所未知的道路。在欧拉之后，数学家纷纷开始探索这片新发现的领地，寻找那些新的联系。

黎曼于 1849 年回到哥廷根，打算在高斯的指导下完成博士论文。这恰好是高斯写信给恩克，谈到自己童年时发现的素数与对数之间关系

---

① 此处指原书第 50 页。



的那一年。虽然高斯在哥廷根与其他同事讲过自己的发现，但是这并非黎曼所想。他正沉迷于从巴黎传来的新数学，打算探索一下赋予虚数的函数世界。

与此同时，柯西开始进行一项工作，就是将欧拉对这片新领地的初步探索进行严格化。虽然法国人是操作方程与公式的大师，但是黎曼决定利用自己从德国教育系统中受到的教育来对这片土地进行更加概念性的研究。1851 年 11 月，他的思想终于成型，他向哥廷根大学提交了自己的博士论文。高斯明显被他的思想打动，他接受了黎曼的论文，并称这是“创造性的、有活力的、真正的数学思想，有着丰富的原创性。”

72

黎曼迫不及待地写信给自己的父亲，述说自己取得的成就，“我相信通过完成论文，我的视野会更加广泛。我希望能尽快学会如何写得更快更流利，特别是在我与人交往的时候。”但是哥廷根的学院生活并不能与柏林那种令人兴奋的生活相比，哥廷根是一所乏味的、孤立的大学。在这里黎曼缺乏自信与那些古老的学术传统交战，并且在哥廷根也没有太多学生可以交流。黎曼不太相信别人，在社交场合也显得很不自然。“他在这里的表现很奇怪，因为他认为所有人都不能容忍他，”同时期的理查德·戴德金（Richard Dedekind）如此写道。黎曼是一个忧郁症患者，经常陷入沮丧的状态。他将自己的脸藏在浓密的大胡子中，因为靠着六个学生自愿交的学费生活，他经常极端忧虑自己的经济。工作与经济的压力导致他的精神状况在 1854 年发生一次短暂的崩溃，然而他的情绪会随着柏林大学的巨星，狄利克雷访问哥廷根而稍微好转。

在哥廷根，黎曼曾试着与著名物理学家威尔海姆·韦伯（Wilhelm Weber）建立友谊。韦伯曾与高斯在许多方面进行过合作，在哥廷根的时候，他们就是科学界的福尔摩斯与华生医生。高斯提供理论支持，韦伯则负责将其应用于实践。他们最著名的发明是认识到电磁学在远距离交流中的作用，并成功地在高斯的天文台和韦伯的实验室之间建起一条电报线路，并通过它来交换信息。

73

虽然高斯认为这项发明只是好奇心所致，但是韦伯清楚地知道这个



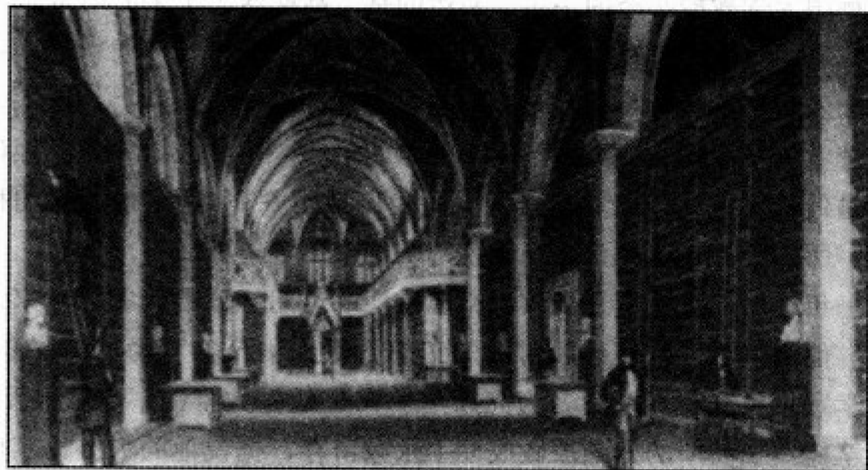


图 17　1854 年前后的哥廷根大学图书馆

发现将最终释放出巨大的能量，“当整个世界被铁路网和电报线路覆盖时，”他写道，“这张网就能像人体的神经系统一样提供服务，前者作为运输的手段，后者则可以以光速来传递思想与感情。”电报的广泛推广以及高斯发明的时钟算法在计算机安全方面的应用，使得高斯与韦伯成为电子商务和因特网的始祖。他们的合作被制成雕像而永存于哥廷根的城市之中。

一位去哥廷根访问韦伯的人如此刻画这位稍显疯狂的发明家，“一位古怪的小个子，声音尖锐使人不快，说话含混不清却又喋喋不休，没有办法，只能耐心地听下去。有时他会毫无来由地笑起来，往往使人感到不知所措。”韦伯比他的合作者高斯要多那么一点反叛的思想，他曾是“哥廷根七勇士”之一，在 1837 年因为反对汉诺威国王专断的规定而被暂时解除教职。在完成自己论文后的一段时间里，黎曼担任韦伯的助手工作，在学徒期间，黎曼对韦伯的女儿产生了些许的感情，但是他的求爱被拒绝了。

1854 年，黎曼写信给他的父亲说：“高斯的病很严重，医生担心他快不行了。”黎曼担心高斯会在审查自己的教职资格之前死去，而那是

成为德国大学教授必经的一步。幸运的是，高斯活了下来并听取了黎曼关于几何的想法，以及他在跟随韦伯工作时产生的将几何与物理联系起来的想法。黎曼认为，所有物理的基本问题都可以由数学得到解答，随后物理学的发展最终证实了黎曼对数学的信心。黎曼关于几何的理论被认为是他最出色的科学贡献之一，而爱因斯坦在20世纪初取得的科学革命，所依赖的支撑平台之一就是黎曼的几何学。

一年之后，高斯离开了人世，但是他的思想却让数代的数学家忙了许久。他留下了关于素数和对数的猜想让后人去证实。为了纪念高斯，天文学家将一颗小行星命名为高斯星。在哥廷根大学的解剖实验室中，你甚至能发现高斯的大脑被做成标本永久留存，据说他的大脑比其他任何人的大脑都要复杂得多。

74

黎曼在柏林大学的老师狄利克雷被任命接替高斯留下的职位。他的到来给哥廷根带来了某种思维上的活跃，这是黎曼在柏林曾经感受过的。一位英国数学家在去哥廷根访问狄利克雷之后，如此描写对狄利克雷的印象，“他个子很高，身材偏瘦，胡须已泛花白……声音尖锐并且有点耳背；那天很早，他刚起床，还没有洗漱与剃须，穿着睡袍拖鞋，拿着一杯咖啡和一支烟。”抛开这种不羁的装扮，狄利克雷是一位追求严格性和证明的人，甚至与他所处的时代不相称。同时期的雅各比在写给狄利克雷的第一个资助人洪堡的信中这样说道，“只有狄利克雷，不是我也不是柯西，更不是高斯，才知道什么是最完美的严格证明，我们都要向他学习。当高斯说他证明了某个命题时，我觉得可能性很小；当柯西这样说的时候，我觉得可能性是一半对一半；但如果狄利克雷这样说，那么肯定就是那么回事。”

狄利克雷的到来给哥廷根的社会结构带来了影响。他的妻子瑞贝卡，是作曲家费力克斯·门德尔松（Felix Mendelssohn）的妹妹，瑞贝卡讨厌哥廷根沉闷的社交气氛，举办了许多的舞会，试图在当地重建她被迫放弃的柏林的沙龙气氛。

狄利克雷不太注重那些不同教育阶层的形式主义，这就意味着黎曼



可以与新来的教授自由地讨论数学问题。从柏林回到哥廷根之后，黎曼曾经非常的孤立，高斯晚年严厉的个性与黎曼的羞怯使得黎曼与这位大师并没有太多的交流。但是，狄利克雷轻松的风格很符合黎曼的胃口，这样更有利于创造两人之间讨论的气氛。黎曼在给父亲的信中谈到了新来的导师："昨天狄利克雷和我在一起两个小时，他阅读了我的论文并且非常友好——考虑到我们之间相差的等级，我几乎不敢相信这一点。"

同时，狄利克雷也很欣赏黎曼的谦逊，并认识到他论文中的独创性。有时狄利克雷甚至将黎曼从图书馆中叫出来，陪他在哥廷根的乡间散步。黎曼在给自己父亲的信中近乎辩解地说这种逃离数学的方法，比起呆在屋里看书，可以使自己更好地进行科学工作。正是他们在下萨克森地区丛林中的某次谈话中，狄利克雷激发起了黎曼的下一个目标，从此素数的研究展开了一个新的层面。

75

ζ函数——音乐与数学之间的对话

在19世纪20年代，当狄利克雷还在巴黎的时候，他就对高斯年轻时的著作《算术探讨》深深着迷。尽管高斯的这本书标志着数论成为一门独立学科的开始，但是其内容很艰深，并且许多地方都不是高斯一贯的简练风格。狄利克雷一段一段的将这本书啃了下来，在晚间他将这本书放在枕头底下，希望第二天能够有所突破。高斯的巨著被描述为"有七个封印的书"，但是由于狄利克雷的勤奋，这些封印都被解开了，其中的宝藏得到了他们应有的广泛传播。

狄利克雷对高斯的时钟计算器很感兴趣，而其中一个由费马注意到的猜想则令他十分关注。如果你取一个表面为N小时的时钟计算器，如果你输入的是素数，费马猜测这个钟将在一点钟敲击无数次。比如说，如果你取一个表面为4小时的钟，那么费马预测将有无数个素数被4除之后余数为1，这些数为5，13，17，29，…

1838年，在狄利克雷33岁时，他证明了费马的直觉是正确的，从



而在数论世界中占有了一席之地。该证明利用了数学中数个不同领域的思想，这些思想初看上去一点关系也没有。不同于欧几里得证明无穷多个素数的巧妙，狄利克雷利用了一个相当复杂的函数，这个函数也是在欧拉那个时期出现于数学领域，这就是 zeta 函数，用希腊字母 ζ 来表示。当给定 x 时，下面的公式给出了狄利克雷当时计算 ζ 函数的方法：

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \cdots + \frac{1}{n^x} + \cdots$$

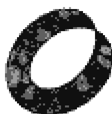
为了计算出结果，狄利克雷需要经过三个步骤。首先，计算指数 1^x，2^x，3^x，…；然后取这些数的倒数（2^x 的倒数就是 $1/2^x$）；最后再将这些结果相加。

76

这是一个复杂的方法。每个自然数 1，2，3，…都在其中起作用，这意味着对于数论学家这个公式有实用性，但是不利方面是你必须要处理无穷项的和。几乎没有数学家认为这个公式会成为一个强大的工具，成为研究素数最好的方法。所有的一切都是偶然得到的。

数学家对于无穷项之和的兴趣来自于音乐，这一点要追溯到古希腊人。毕达哥拉斯最先发现了数学与音乐之间的联系，他通过敲击一个装有水的壶来得到不同的音符。如果他将壶中的水倒去一半再敲击，那么新的音符将比原音符高八度；然后他继续让壶中的水剩下三分之一或四分之一，新产生的音符都与原来的音符产生和弦；而倒掉其他数量的水之后产生的音则与原来的音不和谐。这些听觉上的美是与这些分数紧密联系在一起的，毕达哥拉斯在数 1，1/2，1/3，1/4…中发现的和谐使他相信，整个宇宙是由音乐所控制的，他将此称为“天体的音乐”。

自从毕达哥拉斯发现了数学与音乐之间的算术联系之后，人们就开始比较两者之间的美学与自然特性。法国巴洛克时期的作曲家让-菲利普·拉莫（Jean-Philippe Rameau）在 1722 年写道，“我已经无法忍受那些过去获得的、长久以来就跟随着音乐的经验，我必须承认只有在数学的帮助之下，我的思路才变得清晰。”欧拉设法将音乐理论变成“数学的一个分支，以及找到一个系统的方式，从正确的规则出发，将所有的



一切合适地安排在一起。这样音符的混合也变得使人愉悦。”欧拉相信音符的组合背后一定存在着素数。

许多数学家对音乐有一种自然的喜爱。欧拉常在一整天的辛苦计算之后，以弹钢琴①作为休息。数学系想要成立一个管弦乐团总不是一件难事。在数学与音乐之间有着明显的数字联系，这就是计数在背后作为支撑。莱布尼茨说过，“音乐是人类思想在计数时感受到的快乐，只不过人类并没有意识到这一点。”也许物体之间的共振能更好地说明这一点。

数学是一门关于美的学科，因为美妙的证明和漂亮的结果是大家的共同追求。只有那些拥有特殊美学鉴赏力的人，才能做出数学的发现。数学家渴望的思想火花，就像是在钢琴上胡乱的弹奏之间，突然发现了一些音符组合，其拥有的和谐让它与众不同。

哈代说过他“只对作为创造性艺术的数学感兴趣”。即使是那些在拿破仑时代的大学中任教的法国数学家，做数学的动力也不完全是来自实际应用，而是数学本身的美。做数学研究时感受到的美，与听音乐享受到的美有着太多的共性。如同你反复倾听同一段音乐，以发现错过的共鸣；数学家也在重读证明中找到乐趣，那些证明的微妙之处就在不断的阅读中逐渐地显现出来。哈代相信检验一个证明好坏的标准是看“其中的思想是否被完美和谐地组织在一起。首先验证的就是美，在这个世界上丑陋的数学没有永久的地位。”对哈代而言，“一个数学证明的结构必须是简单清晰的，而不是一盘散沙。”

数学和音乐都有自己特定的符号语言，利用它们我们可以清晰地表达出我们创造和发现的规律。音乐并不仅仅是五线谱上的那些圈圈点点，同样，只有当思想在数学中遨游时，那些数学符号才是有意义的。

正如毕达哥拉斯所发现的，数学与音乐并不仅仅在美学领域有共同点，音乐的物理性质是扎根于数学基础的。当你向一个瓶子吹气的时

① 这里指的是当时的击弦古钢琴。



候，你可以听到一个声音，再稍用力并利用一些技巧，你可以听到一个更高的音——泛音。当音乐家用乐器演奏一个音时，他们其实发出了无穷多的泛音，正如同你在瓶口吹出声音那样。各种乐器依靠这些泛音产生自己独有的音色，因此乐器的物理特征意味着我们听到的是不同的泛音组合。除了基础音符之外，黑管发出的泛音是由那些奇数分母的分数1/3，1/5，1/7…产生；而小提琴的弦，发出的是毕达哥拉斯曾经用自己的壶产生过的，对应于分数1/2，1/3，1/4，…的泛音。

78

一根振动的小提琴弦发出的声音是基础音符与所有可能泛音的无穷和，因此数学家开始考虑数学上的模拟。无穷和 $1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots$ 被称为调和级数[①]，通过将 $x=1$ 代入 ζ 函数，欧拉也得到了这个无穷和。加上越来越多的项之后，虽然这个结果增长得十分缓慢，但是在14世纪人们就已经知道它的最终结果是无穷大。

因此当代入 $x=1$ 时，ζ 函数输出的结果一定是无穷大。然而我们可以不取 $x=1$，当欧拉代入一个比1稍大的数时，结果就不再是无穷大。例如，取 $x=2$ 表示在调和级数中每一项取平方：

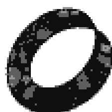
$$\frac{1}{2^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots=\frac{1}{1}+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\cdots$$

这将是一个比较小的数。因为缺少 $x=1$ 时出现的部分分数，欧拉知道这个比较小的数不会发散到无穷，而是在某个固定数处找到归宿。在欧拉那个时代，找到这样的一个无穷和的确切数值并非易事，当时最好的估计是在8/5附近。1735年，欧拉写道，“这个级数已经被研究得太多，几乎不太可能会出现新的结果……我也一样，不管重复努力多少次，只能得到它的估计值。”

但是不管怎样，在他先前发现的鼓励之下，欧拉开始研究起无穷级数。如同将魔方转来转去，欧拉突然发现了这个级数的变化。像魔方表

---

① 调和级数的英文 harmonic series 来源于“和弦”harmony 一词。



面的颜色一样，这些数逐渐组合到一起，形成一个与之前完全不同的模样。欧拉继续写道，“但是现在，非常出乎意料，我发现了一个奇妙的基于圆的面积的公式”——用现代的语言来说，这是一个依赖于 $\pi=3.1415\cdots$ 的公式。

通过一些粗略的分析，欧拉发现这个无穷和最终归于 π 的平方除以6：

$$\frac{1}{1}+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\cdots=\frac{1}{6}\pi^2$$

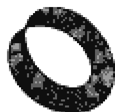
$\frac{1}{6}\pi^2$ 的十进制展开和 π 一样，是完全无序和不可预测的。直到今天，欧拉发现这个潜藏于 $\frac{1}{6}\pi^2$ 之下的规律的方法，仍然是数学中最引人入胜的计算之一，当然也给当时的科学界带来了巨大的影响。没有人会想到单纯的求和 $\frac{1}{1}+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\cdots$ 会与无序的数 π 联系到一起。

这个成功促使欧拉进一步研究 ζ 函数。他知道如果给 ζ 函数代入任何大于1的数，其结果都将是一个有限的数。经过数年孤独的研究，他成功地给出了赋予每个偶数时 ζ 函数的结果。但是对于 ζ 函数仍然有很多不满意的地方，当欧拉代入任何一个小于1的数时，其结果都是无穷。例如 $x=-1$ 时，它将导致无穷和 $1+2+3+4+\cdots$ 这个函数似乎只对大于1的数有效。

欧拉的发现，说明 $\frac{1}{6}\pi^2$ 可以用简单的分数来表示，这也首次说明 ζ 函数可能会揭开数学不同领域之间的某些未曾预料到的联系。欧拉发现的第二个奇怪的联系，与另一个不可预测的序列有关。

重写素数的希腊故事

当欧拉想为自己 $\frac{1}{6}\pi^2$ 的表达式原本粗糙的分析找一个合理的数学基础时，他想到了素数。当他处理这些无穷和时，他回忆起古希腊人的



发现：每个数都可以由素数相乘得到。因此他意识到可以用另外一种方法来重写 ζ 函数。欧拉注意到调和级数的每一项，均能利用素数分解来得到更小的部分，像 1/60 可以写成

$$\frac{1}{60}=\frac{1}{2}\times\frac{1}{2}\times\frac{1}{3}\times\frac{1}{5}=\left(\frac{1}{2}\right)^2\times\frac{1}{3}\times\frac{1}{5}$$

因此调和级数可以不用写成所有分数相加的形式，而是利用那些素数的倒数形成的分数，像 1/2，1/3，1/5，1/7，…等等，然后将它们相乘得到。这个我们今天称为“欧拉乘积”的表达式，将加法与乘法联系在一起。因此在欧拉的新方程中 ζ 函数位于等式的一边，另一边则全部为素数。同样在这个方程中，也说明了每个数都可以分解为素数乘积这个事实：

80

$$\begin{aligned}\zeta(x)&=\frac{1}{1^x}+\frac{1}{2^x}+\frac{1}{3^x}\cdots+\frac{1}{n^x}+\cdots\\&=\left(1+\frac{1}{2^x}+\frac{1}{4^x}+\cdots\right)\times\left(1+\frac{1}{3^x}+\frac{1}{9^x}+\cdots\right)\times\cdots\times\left(1+\frac{1}{p^x}+\frac{1}{(p^2)^x}+\cdots\right)\times\cdots\end{aligned}$$

初看上去，欧拉乘积对于我们研究素数没有任何帮助，毕竟它只是将古希腊人在 2000 多年前已知的结果换了一种表示方法。实际上，欧拉自己也没有抓住重写这个素数性质所包含的全部意义。

直到 100 多年后，欧拉乘积的意义才被狄利克雷与黎曼的洞察力发现。旋转这颗古希腊的宝石，用 19 世纪的眼光来观察，一个古希腊人永远也无法想到的、全新的数学世界出现了。在柏林，狄利克雷发现了欧拉曾经用 ζ 函数来表示素数的一个重要性质——这是古希腊人早在两千多年以前已经证明的结果。当欧拉将 $x=1$ 代入 ζ 函数，结果 $1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots$ 发散到无穷大。欧拉同时发现只有其中出现无穷多素数时，结果才会发散到无穷大。认识到这一点的关键就是欧拉乘积，它联系着 ζ 函数与素数。虽然希腊人在数世纪之前已经证明存在着无穷多的素数，



但是欧拉新颖的证明中包含了与欧几里得完全不同的概念。

有时将熟悉的事物用另一种语言表达出来，往往会有新的帮助。欧拉的新配方促使狄利克雷利用 ζ 函数来证明费马的预言：在一个时钟计算器上，会有无穷多的素数敲击一点钟。欧几里得的思想对证明费马的猜测毫无用处，而欧拉的证明却让狄利克雷灵活地计算出只有素数可以敲击一点钟。事实也确实如此，狄利克雷是第一个利用欧拉的思想来发现新的素数结果的人。这对于理解这些独特的数是一大进步，但是离最后的圣杯仍然很遥远。

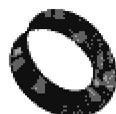
随着狄利克雷来到哥廷根，他对于 ζ 函数的兴趣最终会影响黎曼，只是一个时间问题。也许狄利克雷对黎曼说过这些无穷和的能量，但是黎曼仍然沉浸在柯西那些奇异的虚数世界中。对他而言，ζ 函数只是另外一个可以将虚数代入的函数而已，就像当时大家都在做的那样。

81

然而，一个全新的世界出现在黎曼的眼前。随着他桌子上堆积的演算纸越来越多，他也越来越兴奋。他发现自己陷入了一个虫洞，从抽象的虚数世界被带到了素数的世界。他找到了一种方法，能够解释为什么高斯猜想的素数个数是那么的精确。利用 ζ 函数，解决高斯素数猜想的关键已经掌握在了黎曼的手中。高斯的猜想将会变为高斯所渴望的证明，数学家将最终证明在高斯对数积分与真实素数个数之间的百分差距，确实是随着数的增大而减小。黎曼的发现远不止此，他正站在一个全新的角度来观察素数，ζ 函数演奏的音乐将揭露素数的秘密。

由于曾在学校受到过完美主义性格的折磨，黎曼差点没有记录下自己的发现。他深受高斯的影响，只有完美无缺陷的证明才能被发表。即便如此，他仍感觉到是被强迫解释他所听到的新音乐。当时黎曼刚人选柏林科学院，作为新成员必须报告他们最近的研究结果，这就促使他基于这些新想法写成一篇论文。这将是一种合适的方法，来向科学院表达他对狄利克雷对自己的影响以及作为一名博士生在此两年时间的感谢。毕竟是在柏林他了解到了虚数的力量，从而开辟了新的世界。

1859 年 11 月，黎曼在柏林科学院的院报上发表了自己的发现。这



份十页长的的论文是黎曼仅有的一篇关于素数的文章，但却给该领域带来了深远的影响。通过 ζ 函数这面镜子，黎曼看到了变形后的素数。黎曼的论文就像《爱丽思漫游奇境》中的兔子洞，将数学家领到一个全新的、与直觉相反的数学世界中。在随后的日子里，数学家逐渐掌握了这种新的角度，他们开始理解黎曼发现的必然性和卓越性。

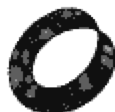
82

除了想像力之外，这份十页的论文非常令人失望。黎曼与高斯一样，经常在论文中隐藏原先的痕迹。对许多结果，黎曼只是声称已经得到证明，但是尚不适合发表。就某种程度而言，考虑到其中包含的缺陷，黎曼能发表这篇文章已经算是奇迹。如果黎曼推迟发表这篇文章，我们将永远无法知道这个猜想，特别是黎曼承认他也无法证明。这个问题的描述被隐藏在这篇十页论文的隐秘之处，不过今天这个问题的答案有了价格——100 万美元，这就是黎曼假设。

不同于文章前面提到的那些断言，黎曼在涉及自己的猜想时，也毫不隐瞒自身的弱点："我应当给出一个严格的证明，但是在数次徒劳尝试之后，我不得不先将它搁置一旁，因为这并非我当下要完成的目标。"他提交给柏林科学院的论文的目标是证明高斯给出的函数，将随着数越来越大时给出越来越好的近似。不过他已经发现了能够最终生成高斯素数猜想的工具，即使目前还无法企及。也许黎曼并没有给出所有的答案，但是他的论文指出了研究这个领域的全新方法，并一直延续到了今天。

尽管狄利克雷对黎曼的发现很感兴趣，但是他仍然于论文出版前的几个月，也就是 1859 年 5 月 5 日，离开了人世。黎曼所获得的回报就是大学里的教职，那个高斯和狄利克雷曾经坐过的位置。

83



第四章

黎曼假设：从随机素数到规则零点

> 将素数分解为音乐，这就是黎曼假设的数学结论。对这个数学定理诗意化的描述就是素数本身拥有音乐，并且还是后现代的音乐。
>
> ——麦克尔·贝里（Michael Berry），布里斯托大学

虽然古希腊人在2000多年前就开始研究素数，但是他们怎么也不会想到，黎曼发现的这条道路，将他们从熟悉的数的世界带往完全陌生的一种数学中。像数学炼金师一样，黎曼只是简单地将虚数和ζ函数混合在一起，没想到从这个混合物中浮现出的竟然是数代人苦苦寻求的结果。他将这一结果写成十页的论文，并意识到这一思想将会在素数领域开辟全新的世界。

黎曼能够释放ζ函数的能量，完全得益于他在柏林以及在哥廷根的博士研究期间做出的关键发现。毕竟高斯在拆除虚数概念的脚手架时，曾将自己思想上的图像表现在这些虚数上。因此高斯在审阅黎曼的论文时，已经感觉到这个年轻人在将虚数代入函数时表现出来的强烈的几何直觉。柯西曾认为一个函数就是一个方程，尽管黎曼关于虚数函数的理论以柯西的工作为出发点，但是黎曼的新思想则认为，即使方程很重要，但是该方程所定义的图像的几何性质才是真正起作用的。

问题在于被赋予虚数的函数，它的图像有时无法画出。为了画出这样的图像，黎曼需要在四维空间中进行想象。对数学家而言，什么是四维空间呢？读过宇宙学家霍金著作的人也许会回答“时间”。其实我们只是用维数来描述那些我们感兴趣的对象，在物理学中，用前三维描述



空间，第四维描述时间。经济学家则愿意用四维空间来探究利率、通货膨胀、失业人数和国债之间的经济学关系。当利率上升时，他们就会研究其他三者相应的变化。虽然我们无法真正地描绘一幅四维经济学模型的图景，但我们确实可以分析出其中的山脉和峡谷。

84

对黎曼而言，ζ函数可以用相似的四维图景来描述。其中两维用来描述作为输入数的虚数坐标，另外两维用来记录这个函数输出的虚数的坐标。

问题在于，人类生活在三维空间中，无法利用现实世界来理解这种新的“虚数图景”。数学家可以利用数学语言，训练自己的思想“看到”这样的结构。但即使缺少这样的数学工具，仍然有方法帮助人们理解这些高维世界，其中一种很好的方法是观察阴影。我们自身是三维物体，可是我们的影子却是二维图像。某种角度的阴影无法给我们提供更多的信息，不过另外一些角度，比如说通过观察侧影，就能得到关于我们三维身体的许多信息。基于同样的原理，对于黎曼建立的ζ函数的四维图景，我们可以构造一个恰当的三维阴影，它保留了足够多的信息，从而我们就能理解黎曼的思想。

高斯的虚数平面图记录了我们输入的那些虚数，南北向的数轴表示我们在虚数部分偏移多远，而东西向的数轴则记录了实数部分。将这样的虚数图平放于桌面上，我们需要做的就是在桌面上方建造一幅物理图景，这样ζ函数的阴影就成为我们可以探索的实在的山峰与峡谷。

每个虚数上方的高度应该记录了该数被输入ζ函数之后的返回值。如同阴影只能表现三维物体很有限的信息一样，在这样的图景中也有不少信息会丢失。旋转原先的物体，可以得到不同的阴影，从而得到不同的信息。因此我们有着多种选择，来确定桌面每个虚数上方的高度。然而，确实有一种角度，其对应的阴影保留了足够多的信息，使得我们可以理解黎曼的发现，同时这也正是黎曼穿过镜中世界时采取的角度。那么，ζ函数的这种特殊阴影究竟是什么样呢？

85

当黎曼开始探索这片世界的时候，他发现了几个重要特征。站在这



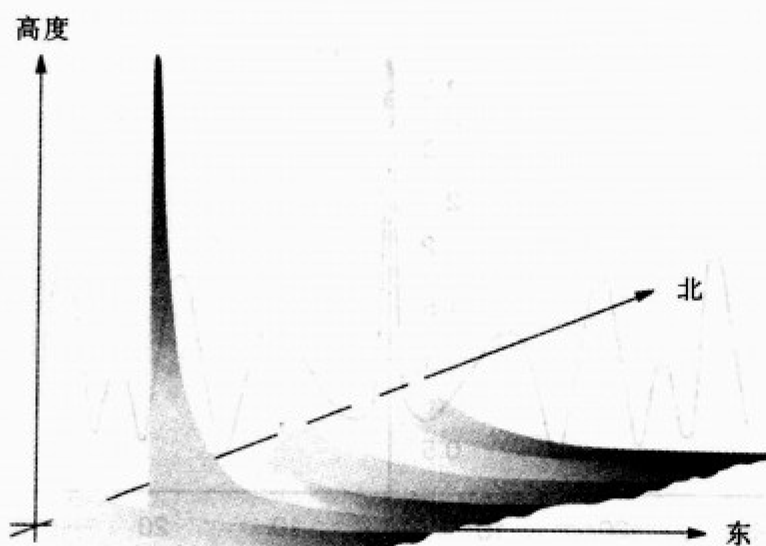


图 18　ζ 世界图像——黎曼发现了如何将这个图像连续地延拓到西部世界

片土地向东方看去，ζ 图像趋于海平面上方一个单位的光滑平面；黎曼转身看向西方，他看到的是一些由南至北蔓延的起伏山脉。这些山脉的峰顶都位于一条直线上，这条直线横穿东西向坐标轴于数 1 处。在交点 1 处的山峰直插入云霄，它实际上是无穷高。这一点欧拉早已注意到，因为将 1 代入 ζ 函数得到的结果是无穷大。在无穷高的峰顶向北或向南看，黎曼可以看到其他的山峰，这些山峰都不是无穷高。其中的第一座山峰位于北方 10 个单位左右的虚数 1 + (9.986…)i 处，高度大概是 1.4 个单位。

如果黎曼将整个世界沿着穿过数 1 的南北向直线切开，观察它的截面图像，得到的应该类似于图 19：

黎曼注意到一个重要的问题。利用 ζ 函数公式，无法建立山脉以西的世界。与欧拉一样，黎曼在为 ζ 函数赋入普通数时碰到了问题。只要输入的数位于 1 以西，ζ 函数公式都趋向于无穷。然而从图像上看，除了那座无穷高山峰之外，其他的山峰似乎都是可以翻越的。

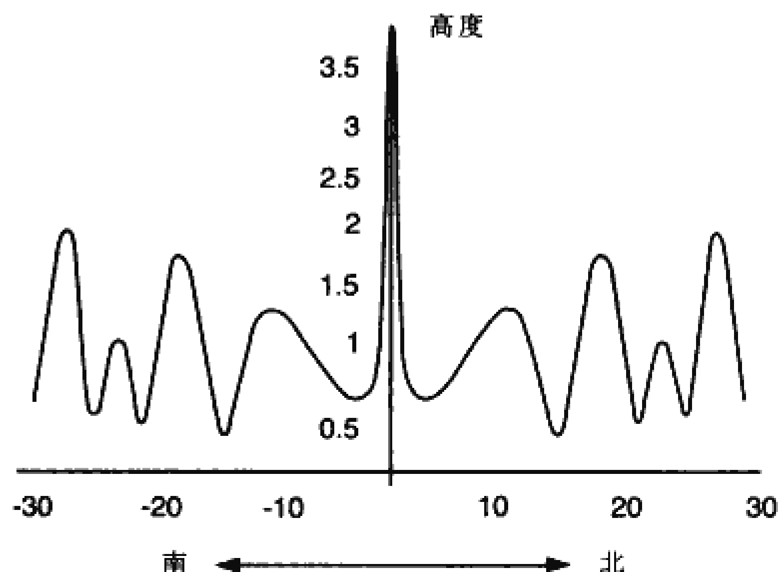
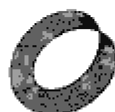


图 19　山脉的横断面图像，位于东西坐标轴上偏东 1 个单位距离处的临界线位置

忽略 ζ 函数的结果，为什么这些山峰无法继续波动下去？显然图像不会就此结束于一条南北向的分割线。在这个界限以西是否真的不存在任何东西？如果你相信方程的结果，你也许会认为 1 以东的图像就是一切，因为方程对于 1 以西的数无意义。黎曼可以完成这幅图景吗？他该如何完成？

幸运的是，黎曼没有被 ζ 函数表面上的棘手所击败。他所接受的教育赋予他的某种能力，正是法国数学家所缺乏的。他相信位于虚数世界之下的方程只是次要的，重要的是实际图像中的四维空间形貌。虽然方程无意义，但是现实中的几何却有意义。最终黎曼找到了另一个方程，可以用来生成丢失的西方世界的图像。新的图像可以完美无瑕地与原先图像拼合在一起，因而虚数世界中的探索者可以从欧拉方程所定义的世界，无阻碍地进入到黎曼新公式定义的世界中，虽然曾经有一道界限横

87



亘在两个世界之间。

有了覆盖整个虚数世界的地图之后，黎曼就可以继续向前进发。在其博士研究期间，黎曼在虚数世界发现两个重要但并非那么直观的事实。首先，他认识到这些虚数有着极其严格的几何意义，对于整个世界只有一种扩张的方法。欧拉所知的东方世界完全决定了西方世界的形状，黎曼不能按照自己的喜好来塑造另一半世界，任何微小的改变都会导致两者交界处的破裂。

虚数世界的不变性是一项惊人的发现。它意味着一旦某个虚数制图师定下了一小块虚数世界，剩下的世界就能被重建。黎曼正是发现了这个事实，即一个区域中的山脉和峡谷包含着整个世界的地形信息。这一点与我们的直觉完全不同，我们完全无法想象，一个真实世界的制图师，只要依靠牛津附近的地图就能恢复整个不列颠群岛的地图。

黎曼做出的关于这个全新数学领域的第二个重要发现，可以被认为是这些虚数世界的 DNA。只需要知道如何在二维虚数平面上标注出那些水平高度恰好位于海平面的点，任何数学制图师都可以重建整个世界，因此标记着这些点的地图就是虚数世界的藏宝图。这真是绝妙的发现！对于一个现实世界的制图师而言，如果你告诉他所有位于海平面的点的坐标，他是绝对无法重建阿尔卑斯山脉的。但是在虚数世界中，使得函数输出值为零的这些虚数的位置告诉了你一切。这些位置因而被称为 ζ 函数的零点。

即使不能访问那些遥远行星，天文学家也能很熟练地分析它们的化学组成部分。那些行星发出的光不仅可以被分光镜分析，而且包含了足够多的关于行星化学成分的信息。这些零点的作用就像化合物发出的光谱。黎曼知道，现在需要做的就是在地图上标记出所有位于海平面的点。这些点的坐标能够提供足够多的信息，来重建海平面以上的山脉和峡谷。

88

黎曼没有忘记探索的出发点。生成整个虚数世界的大爆炸的原点是欧拉的 ζ 函数公式，而该公式可以利用欧拉乘积由素数得到。如果这两



者——素数和零点——生成的是同样的图景，那这两者之间必然存在着某种联系。不同的方法导致了相同的结果，正是黎曼的天才揭示了这两者如何位于同一个方程的两端。

素数与零点

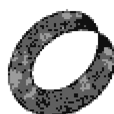
黎曼试图寻找的素数与ζ函数图景中位于海平面的点之间的联系，其直接程度与人们期望的差不多。高斯曾试图估计从1到任意N之间存在多少个素数，利用这些零点坐标，黎曼可以准确地给出从1到任意N之间存在多少个素数。黎曼构造出的公式包含两个重要部分，第一部分是估计小于N的素数个数的新公式R(N)，这个公式从本质上改进了高斯的估计。然而，和高斯的公式一样，这个公式仍然存在着误差。但是经过计算，他发现这个公式给出的误差相当小。举例而言，在小于1亿的数中，高斯的对数积分公式多预测了754个素数，而黎曼的公式仅仅多出97个——这差不多是十万分之一的误差。

下表给出了黎曼的新函数在估计素数个数方面的优越之处，此处N的值从10^2至10^{16}。

虽然黎曼的新函数改进了高斯的结果，但是误差仍然存在。不过，黎曼的虚数世界之旅，让他接触到了高斯从未想象过的某些东西——一种消除误差的方法。利用那些ζ函数图景中被标记出的位于海平面的点，黎曼认识到自己可以校正误差，得到准确的素数个数的公式。这就是黎曼公式中第二个重要部分。

89

N	从1到N的素数个数$\pi(N)$	黎曼的函数R(N)的过估计值	高斯的函数Li(N)的过估计值
10^2	25	1	5
10^3	168	0	10
10^4	1 229	−2	17



N	从1到N的素数个数 π（N）	黎曼的函数 R（N）的过估计值	高斯的函数 Li（N）的过估计值
10^5	9 592	−5	38
10^6	78 498	29	130
10^7	664 579	88	339
10^8	5 761 455	97	754
10^9	50 847 534	−79	1 701
10^{10}	455 052 511	−1 828	3 104
10^{11}	4 118 054 813	−2 318	11 588
10^{12}	37 607 912 018	−1 476	38 263
10^{13}	346 065 536 839	−5 773	108 971
10^{14}	3 204 941 750 802	−19 200	314 890
10^{15}	29 844 570 422 669	73 218	1 052 619
10^{16}	279 238 341 033 925	327 052	3 214 632

欧拉曾惊喜地发现，赋予指数函数虚数值，得到的是一条正弦曲线。一般说来，指数函数的图像是一条迅速攀升的曲线。在引入虚数之后，这条曲线就转变为一条波动曲线，而这类曲线通常与声波相关。欧拉的发现鼓舞了大批人去探索这些虚数引发的奇怪联系，黎曼发现用自己标记着零点坐标的地图，可以将欧拉的结果进行推广。在自己的照虚镜中，黎曼发现利用ζ函数每个零点都能转化为其自身独特的波。每一个波都可以看作是正弦波动函数图像的一个变体。

每个波都由其对应的零点位置决定。位于海平面的点越偏向北方，对应于该点的波振动得越快。如果我们将这个波看作声波，那么这个点越偏北，对应的音符声音越高。

为什么这些波或音符对计算素数个数有帮助？黎曼的发现令人惊讶，他用不同的波高来抵消那些素数个数估计的误差。函数 R（N）已经给出了比较理想的直到 N 的素数个数估计，如果在这个估计上加上数 N



处的每个波高，黎曼发现可以得到准确的素数个数——误差被完全消除了。黎曼终于找到了高斯一直在寻找的圣杯：数 N 以内素数个数的准确公式。

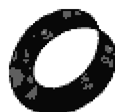
这个发现的公式可以用文字简单地记为“素数 = 零点 = 波”。黎曼用零点表示素数个数的公式，对数学家而言就如同爱因斯坦质能方程 $E=mc^2$ 一样激动人心，它们都是一个关于联系与变换的公式。一步一步地，黎曼目睹了素数的转化。素数构成了 ζ 函数世界，在此世界中位于海平面的点则是揭开素数秘密的关键；然后，这些位于海平面的点又分别产生类似于音符的波，从而出现了新的联系；最终黎曼再次回到他的出发点，表明如何利用这些波去计算素数的个数。当整个事件再现为一个完整的圆时，黎曼肯定也为这个奇妙的变化而吃惊。

黎曼知道，既然存在着无穷多个素数，那么在 ζ 函数世界中肯定也存在着无穷多个位于海平面的点。因此存在着无穷多个波，可以被用来控制误差。下面给出一种图形上的描述，表示了如何通过在黎曼的素数个数公式上加上修正波来改进这个公式的效果。在加上零点处的波之前，黎曼的函数 R（N）的图形（图 20 上图）一点也不像表示素数个数的阶梯状图形（图 20 下图）：一个是光滑的，一个是锯齿状的。

考虑到我们在向北进发时碰到的前 30 个零点，利用它们产生的波来抵消误差之后，黎曼的函数图像发生了改变，对应于 R（N）的光滑图形变成类似于素数个数的阶梯状图形。（图 21）

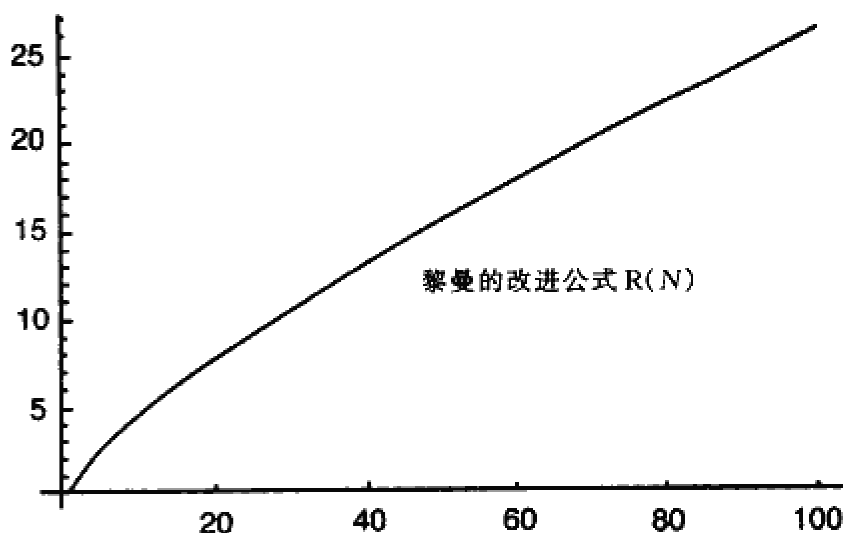
每一个新的波都将原来的光滑图形进行微小的扭曲。黎曼意识到，当你在 ζ 函数图景中向北前进时，每碰到一个海平面上的点就加上相应的波，这样加上无穷多个波之后，最终的图像将与素数个数的阶梯状图像完全吻合。

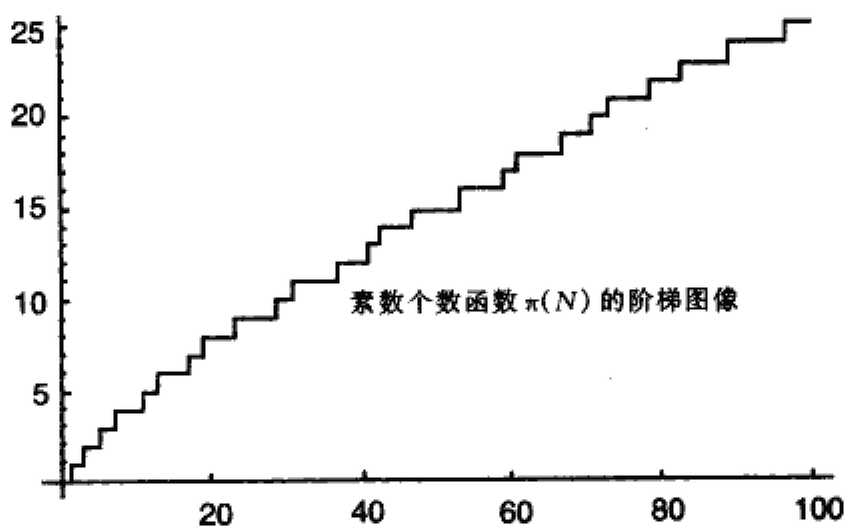
一代人之前，高斯曾经认为他发现的素数硬币是自然界用来确定素数的工具；而现在，黎曼发现的波才是自然界抛硬币的结果。在数 N 处每个波的高度能预测每一次抛出素数硬币之后，得到的是正面还是反面。而高斯发现的素数与对数之间的联系只是预测平均的素数行为。黎



曼发现了是什么控制着素数的微小细节，他揭开了赢得素数彩票的秘密。

91





92

图 20　挑战：如何从上图的黎曼光滑图形得到下图锯齿状的图形

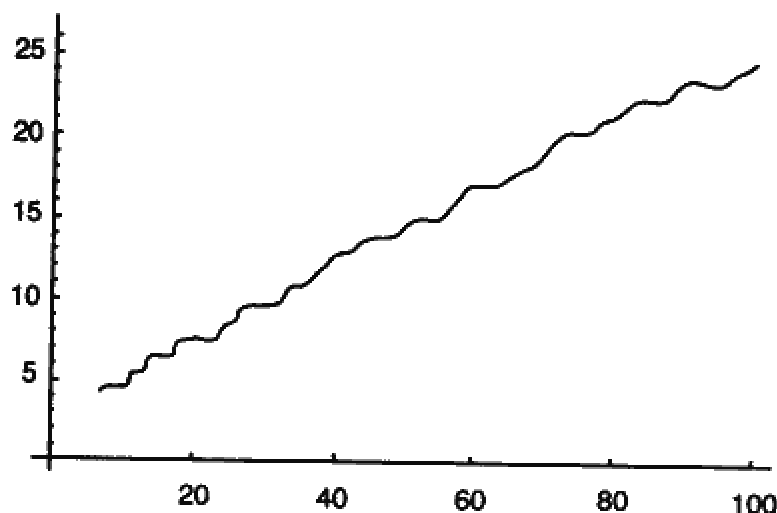


图21　加上前30个波之后的黎曼光滑图形

素数的音乐

数个世纪以来，数学家倾听素数的音乐，但是只能听到无序的杂音。这些素数在数学的五线谱上随意地标点，无任何旋律可言。现在黎曼发现了新的耳朵，通过它可以听到这些神秘的旋律。从 ζ 函数图像中的零点生成的那些类正弦波揭示了某些隐藏的和谐结构。

毕达哥拉斯通过敲击水壶，发现了隐藏在分数序列背后的音乐和弦。素数研究的大师，梅森与欧拉，建立了和声学的数学理论。但是他们都完全没有想到素数与音乐之间存在着直接的联系。这个音乐只有19世纪数学家的耳朵才能听到，黎曼的虚数世界产生了简单的波，这些波组合在一起就能再现素数的微妙和弦。

相比于其他人，有一位数学家更加能理解为何黎曼的公式成功捕获了隐藏的素数音乐，他就是约瑟夫·傅里叶。作为一个孤儿，傅里叶在本笃教会开办的军事学校中接受教育。他一直很顽皮，直到13岁那年



被数学深深地吸引。本来傅里叶注定要做一位修士，但是1789年的政变让他摆脱了大革命前已设定好的生活路线，投身到他热爱的数学和军事中去。

傅里叶是大革命的狂热支持者，不久便受到了拿破仑的重用。拿破仑曾建立不少学院来培养那些能促进他的文化和军事革命的教师和技术人员。在了解到傅里叶不光拥有数学家的才能，而且可以胜任教师的工作之后，拿破仑让他负责高等综合理工学院的数学教育。

拿破仑对傅里叶取得的成就很满意，因此让他加入“文化部队”前往埃及进行战后的“文明化”。这次远征的动机是拿破仑希望借此干扰英国不断增长的殖民霸权，但研究古代世界的计划也在日程表中。从拿破仑的旗舰“东方号”踏上开往北非海岸路程的第一天起，这些知识分子立即投入到紧张的工作中去。每天早晨，拿破仑会向这些学院派大使宣布当天的任务，他们必须在傍晚交出满意的答案。因此，当水手辛勤地操作缆绳与风帆之时，傅里叶和他的同事在甲板下进行辛苦的计算，以解答拿破仑感兴趣的众多问题：从地球的年龄到其他行星是否有人居住等等。

到达埃及并非事情的终结。在1798年的金字塔战争之后，拿破仑用武力拿下了开罗，他很失望地看到埃及人并不感谢傅里叶等人给予的强制性的文化传输。在一次晚间的冲突中，300人被叛乱分子杀死。这促使拿破仑放弃埃及，回到巴黎去处理酝酿中的混乱。皇帝悄无声息地离开，根本没有通知这些知识分子。由于傅里叶的官衔不够高，又不敢冒险逃走，否则会以叛逃罪名处死，所以他被迫留在了开罗附近的沙漠。在法国决定撤出，让英国接手埃及的“文明化”任务之后的1801年，傅里叶才设法回到了法国。

由于在埃及时习惯了沙漠的灼热，傅里叶回巴黎后的居所被朋友们戏称为炼狱。但是傅里叶相信高温可以使身体健康，并且能治愈某些疾病。因此朋友们总是能在热得像撒哈拉沙漠的房间中，找到把自己包裹得像木乃伊一般浑身大汗的傅里叶。



94

傅里叶对热的偏爱也延伸到了学术工作上。他对于热的传播的分析，为他在数学史上占有了一席之地，同时也被英国物理学家开尔文勋爵称为“伟大的数学诗篇”。在此之前的1812年，巴黎科学院宣布设立一项数学大奖，用于奖励揭开热在物质中传播的秘密的人。傅里叶受此激励，最终以其新颖和重要的思想得到认可而获得奖励。但他的工作也受到了勒让德的批评，作为大奖评委会成员之一的勒让德指出，傅里叶的论文包含了许多错误，并且其中的数学解释也很不严格。尽管傅里叶对科学院的批评很生气，但他也知道仍然有许多工作要做。

当傅里叶开始着手改正这些错误时，他首先要理解那些表现物理现象的图形所包含的意义——比如说，随时间变化的温度变化图像、表现声波的图像等等。他知道声音可以用这样的一幅图像来表示：水平轴表示时间，垂直轴用来表示每一时刻的音量和音高。

傅里叶从最简单的声波着手。敲击音叉的时候，你会发现记录下来的声波图像是一条纯正的、完美的正弦曲线。如何用这些纯正的正弦曲线组合成更加复杂的声音，正是傅里叶将要探索的问题。如果小提琴和音叉发出同一个音符，它们的声音听上去差别很大。正如我们在第78页①看到的那样，小提琴弦不光以基本的、由弦长决定的频率振动，同时还存在着其他附加音符，也就是对应于弦长的简单分数的和弦音符。这些附加音符的曲线是更高频率的正弦曲线，它们由最低的、最基本的那个音符决定，它们组合在一起就产生了小提琴的声音，其图像类似于锯子的尖齿。

用单簧管演奏同一个音符的时候，声音却是如此的不同，这又是为什么？单簧管的声波看上去像一些方波函数，不同于小提琴的锯齿状，而是像那些城堡顶部的垛口。产生这种声波的原因是因为单簧管是一端开口，而弦是两端固定。这就是为什么单簧管产生的和弦与小提琴产生的和弦差别如此之大的原因。单簧管声音的图像同样可以由不同频率的

① 此处指原书第78页。



正弦波生成的图像来描述。

傅里叶意识到，即使由整个管弦乐队产生的声音所构成的图像，也可以分解成简单的那些基础正弦波加上不同乐器分别产生的和弦。每个单音又可以用音叉来重现，因此傅里叶证明了同时敲击大量的音叉就可以复原整个管弦乐队的声音。如果蒙上眼睛，你肯定无法分辨哪个是管弦乐队发出的声音，哪个是数千把音叉发出的声音。这也正是 CD 编码的核心原理：CD 告诉喇叭如何振动来发出所有的正弦波，从而组成整个音乐。这些正弦波组合起来，给你的感觉就如同一支管弦乐队正在你的起居室中现场演奏。

95

将不同频率的正弦波组合在一起，产生的可不止乐器的声音而已。像收音机在没有信号下产生的静电噪音或水流声都可以用无穷多个正弦波相加得到。与产生管弦乐声音的特定频率不同，噪音是由某个范围中所有频率的波构成。

傅里叶革命性的思想并没有简单地停留在重现声波这一步，他试图利用正弦波去描述更多物理和数学现象。与傅里叶同时期的人普遍怀疑，像正弦图像这么简单的图形能用来描述管弦乐队产生的复杂声波或者水流的声音。一些法国的著名数学家也强烈反对傅里叶的思想。但是依靠着自己与拿破仑的关系不错，傅里叶并不害怕挑战这些权威人士。他说明了如何通过选择一些以适当频率振动的正弦波来构成整个复杂的图像。如果你将这些正弦波的高度相加，同样可以得到这样的图像。基于同样的原理，CD 唱片将多个纯音符的音叉组合在一起，产生了复杂的音乐。

这也正是黎曼在他的十页论文中成功做到的东西。将那些对应于 ζ 函数图像中零点的波函数相叠加，黎曼准确地得到描述素数个数的阶梯函数。傅里叶立刻就意识到，黎曼发现的素数个数的公式就是描述素数音乐的基本音符，素数音乐就是复杂的阶梯函数。那些由 ζ 函数图像中位于海平面的零点产生的波，就像是音叉发出的、不含任何和弦的纯音符。当这些基本的音符被同时奏响时，产生的就是素数的音乐。那么这

96



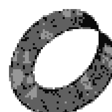
个素数的音乐听起来如何？是像管弦乐队的声音，还是像水流产生的噪音？如果黎曼的这些音符频率是在一个连续的范围之内，那么素数产生的就是噪音。但是如果这些频率代表着独立的音符，那么素数产生的则是类似于管弦乐队的声音。

由于素数的随机性，我们觉得这些由零点产生的音符组合起来只能是噪音，而不会是其他什么东西。每个零点的南北坐标决定了音符的音高。如果说素数产生的确实是噪音，那么在 ζ 函数的图像上，肯定会出现零点的集中地带。由黎曼提交给高斯的论文知道，如果真的存在这么一个零点的集中地带，那么整个图像将被迫处于海平面。但实际图像并非如此，所以素数的音乐不可能是噪音。由于海平面上的点肯定是独立的点，因此它们产生的是一系列独立的音符。从而在素数中，大自然隐藏了一首由数学管弦乐团演奏的音乐。

黎曼假设——混沌中的有序

从虚数世界的图像中将那些位于海平面的点挑出来，如同某件数学乐器发出的音符一样，对每个点构造一个波函数。将这些波函数组合到一起，黎曼就得到了一个能够演奏素数音乐的管弦乐队。位于海平面的点的南北坐标决定了波的频率——也就是对应声音的音高；另一方面，欧拉早已经发现，点的东西坐标决定了每个音符的音量。音符的音量越大，其对应的波动图像振幅越大。

黎曼想知道是否存在这样一个零点，它对应的音符所发出的音量比其他零点对应的音符的音量更响亮。这样的一个零点产生的波形，它的振幅将明显高于其他所有的波。因此它在计算素数个数的过程中起着最大的作用，因为波的高度影响着高斯的估计和真实素数个数之间的差距。在这个素数管弦乐队中是否存在某件乐器，它作为独奏乐器，作用要高于其他乐器？如果一个位于海平面的点，它的坐标越往东，则对应的音符音量越大。为了掌握整个乐队的平衡，黎曼必须回到他的虚数图



像中确定每个零点的坐标。

值得注意的是，直到目前为止，黎曼所有的研究都没有涉及位于海平面的点的位置。有一些零点很容易被找到，但是它们对素数的音乐不起作用，因为它们没有音高。因此数学家将它们称为平凡的零点。黎曼所要寻找的就是除此之外的那些零点。

当黎曼开始寻找这些零点的确切位置时，碰到的事情令他十分惊讶。黎曼计算的那些零点，并非随机分布于整个图像中发出或高或低的音量，而是奇迹般地落在一条南北向的直线上。看上去那些位于海平面的点都具有相同的东西坐标——1/2。如果这是真的，就意味着这些对应的波也具有相当完美的平衡，不会出现参差不齐。

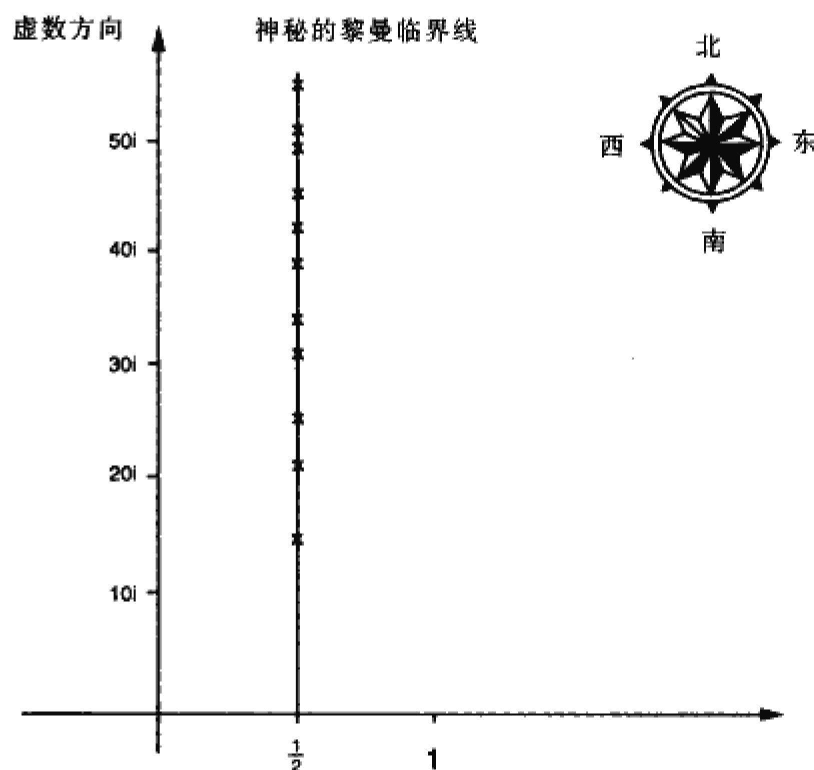


图 22　黎曼的素数藏宝图——小叉号代表 ζ 函数图像中位于海平面的点的位置



黎曼计算的第一个零点的坐标为(1/2, 14.134725…)，这意味着从坐标原点偏东1/2，偏北14.134725。下一个零点的坐标为（1/2, 21.022040…）（至于黎曼如何计算这些零点的坐标，到现在仍然不甚清楚）。看上去这些零点并非随机分布，黎曼的计算表明它们似乎是沿着某条直线有序的安排。黎曼猜测他所能计算出的零点出现这样的共性并非巧合，他相信海平面上的每个点都位于这条直线之上，这就是黎曼假设。

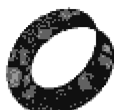
穿过分割了数的世界与ζ函数世界的镜子，黎曼看到了素数的镜像，看到了混乱分布于镜子一边的素数，转变为另一边严格有序排列的零点。数世纪以来，数学家凝视素数，期望能从中发现某种神秘的规律，最终，黎曼做到了这一点。

这个规律的发现完全出乎意料。黎曼很幸运地成为了那个出现在正确时间、正确地点的人：他完全不知道镜子另一边有什么在等着他。然而在那里的东西确实彻底改变了理解素数神秘性的任务。现在数学家有了新的领域可以探索，如果他们能确定那些位于海平面的点，他们就能揭示素数的奥秘。同时，黎曼还发现了某些穿过整个图像的特征线(ley line)，它们在数学中占据着重要的作用，这一点从它的现代名称——临界线——就可以得到说明。现在，现实世界中随机的素数问题，已经转化为寻求理解虚数世界中的音乐的问题了。

由于存在着无穷多的零点，黎曼对少数几个点的零碎结果还不足以建立一套理论。同时，黎曼知道这条临界线有着重要的意义。他已经知道东西向数轴是整个图像的一条对称轴，北方的任何行为都会在南方反映出来；更进一步，黎曼发现了更重要的结果，穿过坐标1/2的南北向直线也是图像的一条对称轴。这一点更让黎曼相信，自然界会利用这条对称轴来安排所有的零点。

99

要特别指出的是，在黎曼向柏林科学院提交的有关这个重要发现的论文中，并没有涉及他对于那些零点坐标的计算结果。当然你也很难从这篇论文中找到这样的论述，他只是说许多零点似乎位于某条直线上，



并且有很大可能，所有的零点都位于该直线上。但是黎曼承认，他并没有花大力气来证明这个假设。

毕竟，黎曼是在证明一个更加直接的结论——高斯的素数猜想：为什么考虑的素数越多，高斯的素数个数公式就越准确。黎曼知道，虽然这个证明难以捉摸，但是只要他关于临界线的猜测成立，就意味着高斯猜想成立。高斯公式的误差可以用每个零点的位置来描述，当一个零点越偏向东，波的音量就越大，从而误差越大。这也是为什么黎曼关于零点位置的预测如此重要的原因，如果这个预测正确，所有的零点都位于这条神奇的临界线上，那么高斯的猜想将会永远正确。

这份十页论文的出版标志着黎曼的一段快乐时光，他被任命接替他的导师高斯和狄利克雷曾担任的教职。支持他的哥哥在 1857 年去世之后，他的妹妹来到哥廷根陪伴他。有了亲人的陪伴，黎曼的精神得到了好转，他不再像过去那样处于消极状态。同时，拥有了教授职位，他摆脱了学生时期的穷困，可以买一幢像样的房屋以及雇佣管家，从而他有了更多的时间来研究那些一直在脑中盘旋的想法。

不过后来黎曼再也没有做过任何素数问题。利用自己的几何直觉，黎曼发展了一套空间几何学，后来这门几何学成为爱因斯坦相对论的基础。他与妹妹的好友伊莉斯·科克（Elise Koch）在 1862 年结婚，这成为他好运的巅峰。一个月之后，黎曼因为胸膜炎病倒，从此病魔一直纠缠着他。许多次他到意大利的乡下疗养，特别是比萨，那是他唯一的孩子伊达 1863 年 8 月出生的地方。黎曼喜爱去意大利休养，并非仅仅因为那里温和的气候，良好的学术环境也是一个重要原因，在当时，意大利数学界最能接受他的革命性的新思想。

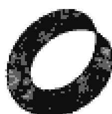
100

黎曼最后一次来到意大利，并非是想逃离哥廷根沉闷的环境，而是因为军队的侵略。1866 年，汉诺威和普鲁士的军队入侵哥廷根，黎曼被困于居住地——位于城外的高斯天文台。在判断了形势之后，黎曼很快逃到了意大利，这件事对他脆弱的性格造成了很大的打击。在出版了关于素数的论文之后 7 年，黎曼死于肺病，年仅 39 岁。

面对黎曼留下的杂乱住所，管家清理了他许多未发表的手稿，直到被哥廷根的职员制止。剩下的手稿被送给黎曼的遗孀，从此消失了数十年。大家猜测，如果管家不是那么尽职地清理房屋，也许能留给我们更多的东西。黎曼在他的十页论文中曾说，他相信自己可以证明绝大多数的零点位于临界线上，但是他的证明尚不适合发表，因此不能详细阐述。这个证明一直没能从他未发表的论文中找到。直到今天，数学家也不能重现该证明。这些失踪的手稿与费马声称找到了大定理的证明一样，成为数学中的传说。

那些从管家的火焰中幸存的未发表论文于50年之后重现世间。令人失望的是，它们表明黎曼曾证明了大量结果，但是都没有发表。文章中列举的结果，暗示着黎曼曾经有过许多想法，只是它们都消失于热心管家的炉火之中，再也无法面世。

101



第五章

数学接力赛：黎曼革命的实现

数论中的问题如同艺术珍品一样不朽。

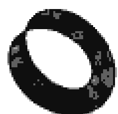
——大卫·希尔伯特，雷·威尔伯·瑞德（Legh Wilber Reid）《代数数论基础》序言

从亚历山大的欧几里得，圣彼得堡的欧拉，到哥廷根三剑客——高斯、狄利克雷和黎曼，素数个数问题如同接力棒一样由上一代传给下一代。每个人带来的新观念都推动着这个问题的前进，数学的潮流也在素数上留下了各自独有的印记，代表了当时特别的文化风貌。黎曼的贡献如此超前，以至于直到30年后才有人可以理解他的新思想。

时间到了1885年，看上去游戏已经结束。虽然在一个世纪之前，信息在全球之间的传播速度远不如邦比艾里的愚人节电子邮件那么快，但是有消息称，某个不知名的人物不光接过了黎曼的接力棒，而且已经冲过了终点线。荷兰数学家托马斯·斯第吉斯（Thomas Stieltjes）声称他已经给出了黎曼假设的证明，证实了所有零点确实都位于黎曼的那条穿过1/2的临界线上。

但是斯第吉斯并不具有胜利者的潜质。在学生时期，他有三门大学课程没有通过，这令他在荷兰议会任职，并担任鹿特丹大坝工程总工程师的父亲十分失望。不过这并不是因为斯第吉斯偷懒，而是在莱顿大学图书馆阅读纯数学的乐趣使他分了心，没有能好好准备那些考试的习题。

斯第吉斯最喜欢的作者是高斯，他希望能跟随大师的脚步。他像高



斯在哥廷根大学天文台一样，在莱顿大学天文台获得了一个职位。不过他永远也不会知道，如果不是他有名望的父亲和天文台负责人打过招呼，这个职位也不可能给他。当他的望远镜在天空巡视时，他的乐趣并非在于确定新星的位置，而是天体运动中蕴涵的数学。当他的思想成熟之后，他决定写一封信给当时法国学术界著名的数学家查尔斯·厄米特(Charles Hermite)。

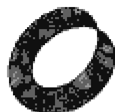
102

厄米特生于1822年，比黎曼大4岁，当时正好是60岁，他也是柯西和黎曼所从事的复变函数领域的领军人之一。柯西给厄米特的影响并非只有数学，厄米特年轻时是一位无神论者，虔诚的罗马天主教徒柯西在厄米特的一次重病期间，影响了他脆弱的思想，将他转变为一个天主教徒。其结果则是某种数学与神秘主义的奇怪混合，类似于对毕达哥拉斯的崇拜，厄米特相信数学的存在是某种超自然的状态，只允许人类数学家偶尔偷偷看到一隅。

也许这正是为什么厄米特能热情地的回信给一位莱顿大学天文台的小助理，使他相信自己是被赐予更高数学能力的人。不久，两人开始了热烈的数学通信，在12年的时间中有432封之多。虽然斯第吉斯没有任何学位，但是他的思想仍然给厄米特留下了深刻印象，厄米特尽量地给予斯第吉斯帮助，并允诺他得到图卢兹大学的教授职位。在给斯第吉斯的一封信中，厄米特这样写道：“Vous avez toujours raison et j'ai toujours tort.（你总是正确，而我总是错误。）”

正是在这些通信中，斯第吉斯宣称他证明了黎曼假设。由于厄米特对这位年轻门生的信心十足，根本就没有怀疑斯第吉斯是否真的给出了证明。毕竟，斯第吉斯已经在数学的其他方面做出了巨大贡献。

由于黎曼假设出现的时间不长，不像现在这样已经演变为世界公认的难题，斯第吉斯的声明也不像现在那样会受到热烈的关注。另外黎曼并没有正式提出这个假设，而是将它深深地隐藏在那份十页的论文中，同时也没有太多其他的信息。这就需要下一代人才能领略黎曼假设的重要性。然而斯第吉斯的声明同样令人兴奋，因为证明了黎曼假设，就可



以证明高斯关于素数个数的猜想，而在当时高斯猜想是数论中的圣杯。对于 1 000 000 以内的数，高斯对于素数个数的猜想与标准值相差百分之 0.17，而对于 1 000 000 000 以内的数，这一误差为百分之 0.003。高斯相信，当数变得越来越大时，百分误差也将会越来越小。到了 19 世纪后期，高斯猜想已经十分有名，征服它的人将一举成名。而实际计算的结果也充分说明高斯猜想正确的可能性很高。

在斯第吉斯提交证明给厄米特之前，对高斯猜想的最好结果是 1850 年左右由欧拉在圣彼得堡的继承者做出。俄国数学家帕努梯・切比雪夫（Pafnuty Chebyshev）并不能证明高斯猜想与实际素数个数之间的百分误差会越来越小，但是他证明了无论你选多大的数 N，在 N 以内的素数个数的百分误差不会超过 11。看上去，这与高斯对于 100 万以内的素数个数做出的估计误差 0.03% 相差甚远，但是切比雪夫的结果成功地保证了，无论你选择多大的数，这个百分误差也不会突然变得很大。在切比雪夫的结果之前，高斯的猜想仅仅是建立在一些数值实验的基础之上，切比雪夫在理论上的分析首次保证了在对数与素数之间存在着某种联系。然而，证明这个联系仍然有很长一段路要走，这与高斯提出猜想的难度基本相当。

切比雪夫利用纯基础的方法成功地控制了这个误差。在哥廷根奋战于复数世界中的黎曼也听说了这项工作，这从一封黎曼打算寄给切比雪夫的信中可以看出端倪，他在信中向切比雪夫介绍了他自己的工作。在黎曼遗留下来的手稿中还包括了几份特殊的手稿，在其中他试图正确拼写出切比雪夫的名字。至今我们也不知道黎曼是否将这封信寄给了切比雪夫，但是无论怎样，切比雪夫在素数个数的误差估计上没有做出更进一步的结果。

这也正是斯第吉斯的声明给当时的数学界带来惊喜的原因。当时并没有人能想到黎曼假设是如此难以证明，但是证明高斯猜想确实是一项了不起的成就。厄米特急切地想看到斯第吉斯的详细证明，但是年轻人却显得有些勉强，认为证明尚未完善。在随后的 5 年中，虽然厄米特不



断地催促，斯第吉斯还是不能拿出一些东西来支持他的声明。由于斯第吉斯仍然不愿意解释他的思想，厄米特的失望与日俱增。为了消除这种感觉，他决定使用一个计策来激出这个证明。厄米特决定将 1890 年巴黎科学院的数学科学大奖授予证明高斯素数猜想的人，他相信这个奖非自己的朋友斯第吉斯莫属。

104

这就是厄米特的计划：为了赢得这个大奖，斯第吉斯仅仅宣称解决了黎曼假设是不够的。更为合理的是，他只需要考虑虚数世界中的一小部分——欧拉部分与黎曼扩张部分的边界，只需要证明没有零点落在这条穿过 1 的南北向的边界线上，就可以完成整个证明。黎曼扩张部分可以用来决定高斯公式中的误差，该误差由这个部分中零点的偏东程度决定，零点越偏向东边，误差则越大。如果黎曼假设成立，那么这个误差将非常小。但是如果黎曼假设不成立，高斯猜想也可能正确——只需要所有的零点都严格位于穿过 1 的南北向边界线的西方就可以。

大奖的截止日期到了，斯第吉斯仍然保持沉默。本来厄米特非常失望，但出乎他意料之外的是他的学生雅格斯·哈达马（Jacques Hadamard）提交了一份解答。虽然这份解答离完全证明还有相当大的距离，但是哈达马的新思想已经足以使他获得这份奖金。受此激励，哈达马在 1896 年补上了这个新思想中的漏洞。尽管他还不能证明所有的零点都位于穿过 1/2 的那条黎曼临界线上，但是他证明了所有零点都无法越过那条穿过 1 的边界线。

终于，在高斯发现素数与对数函数之间的关系一个世纪之后，数学中终于有了一个关于高斯素数个数猜想的证明，从此这个猜想变成了著名的素数定理。自从希腊人证明了存在无穷多个素数以来，这个证明是关于素数的最出色结果。哈达马证明了，尽管我们永远也不能到达数的尽头，但是不会有异常情况等待着旅行者，早期高斯的实验证据也不是大自然为了误导我们而耍的花招。

如果没有黎曼的起步工作，哈达马就不可能取得这个成就。虽然哈达马的证明思想基于黎曼对 ζ 函数图像的分析，但是他离证明黎曼假设



还很远。在他阐述证明的论文中，哈达马承认自己的工作无法与斯第吉斯的成就相比。直到 1894 年去世，斯第吉斯仍然宣称自己已经得到了黎曼假设的证明，因此他也位于那些只闻其声、不见其实的知名数学家之列。

不久，哈达马发现自己不能独享证明素数定理的荣誉，因为在同时，一位比利时数学家查尔斯·德·拉·瓦勒普桑（Charles de la Vallee-Poussin）也独立地给出了一个证明。哈达马和瓦勒普桑的巨大成就标志着一段新路程的开始。在这段一直延续到 20 世纪的路程中，数学家渴望在黎曼开辟的世界中进行各自的探索，而哈达马和瓦勒普桑已经建立了向黎曼的临界线进发的大本营。也正是在这一时期，黎曼假设成为了数学探索的珠穆朗玛峰，而它的证明则依赖于那些 ζ 函数世界中的最低点。既然高斯素数定理已经得到了解决，现在是让黎曼假设从那篇提交给柏林科学院的精深论文中现身的时候了。

105

正是另一位哥廷根的学者，大卫·希尔伯特（David Hilbert）将黎曼非凡的洞察力带到了世人的面前。这位传奇般的数学家带动了 20 世纪的潮流，令黎曼假设成为数学界的终极目标。

希尔伯特：数学吹笛者①

由于欧拉于 1735 年解决了著名的七桥问题，普鲁士的柯尼斯堡在 18 世纪数学界中声名远扬。而在 19 世纪后期，这个小镇再次留名于数学界，因为它是 20 世纪的数学巨匠希尔伯特的出生地。

尽管热爱自己的故乡，但希尔伯特知道在哥廷根的城墙之内数学火焰燃烧得最旺。由于高斯、狄利克雷、戴德金以及最重要的黎曼等人的

---

① 源自 19 世纪英国诗人布朗宁（Robert Browning）的童诗“The Pied Piper of Hamelin”，传说德国不伦瑞克（Brunswick）地区的哈麦林城（Hamelin）突然闹出鼠患，一位异客利用自己的笛声将老鼠吸引到河中，落水而亡，从而消除了鼠患。后因市长拒付约定的报酬，异客再次利用自己的笛声将城中所有儿童都带至山中，从此消失不见。

努力，哥廷根已成为数学家心目中的麦加。也许与同时期的人相比，希尔伯特对黎曼为数学带来的巨变体会更深。黎曼认为理解数学世界底层的结构和模式，比起简单关注于公式和枯燥的计算更加有趣。从此，数学家以另外的方式来倾听数学的音乐——不再关注于单独的音符，而是试图听到研究对象背后的旋律。黎曼为数学思想带来的复兴，一直延续到希尔伯特这一代人。希尔伯特在1897年写道，他试图实现黎曼的准则，根据这个准则，证明应该是由思想决定而不是由计算决定。

正因如此，希尔伯特在德国的学术领域中奠定了自己的地位。他从学生时代就知道希腊人证明过存在着无穷多个素数，这些素数构成了所有的自然数。希尔伯特知道如果关注方程而不仅仅是数字，事情将完全改观。到了19世纪末，能否像素数生成所有自然数一样，存在有限多个方程，由它们可以生成某类无限多的方程，已经成为了一个挑战。与希尔伯特同时代的数学家试图通过辛苦地构造这些方程来证明这个结论，而希尔伯特的证明令他们大吃一惊：即使不能构造出这有限多个方程，也可以证明这有限多个方程肯定存在。如同高斯的老师不相信学生巧妙地将1至100进行相加一样，希尔伯特的前辈也深深怀疑没有严格验证，怎么能解释这样的方程理论。

106

这是对当时正统数学的挑战。在你没有看见某个有限集合时，即使证明了它确实存在，你也无法接受它的存在性。你看不见某物，但是却被告知它确实存在于那里，这对于当时还恪守于传统具体方程和公式的法国数学家而言，是令人惶恐的一件事。作为该领域的专家，保罗·戈旦（Paul Gordan）认为希尔伯特的工作“不是数学，而是神学”。虽然如此，希尔伯特仍然没有改变自己的想法，最终证实希尔伯特是正确的。戈旦不得不让步，“我相信神学也是有优点的。”后来希尔伯特投身于数论的研究，一门被他形容为“美与和谐的统一体”的学科。

107

在1893年，希尔伯特应德国数学会的要求，计划写一篇有关世纪末数论研究现状的论文，这对于一位30刚出头的人而言实在是要求过高。100年前，这个学科还未成形，高斯出版于1801年的《算术探讨》



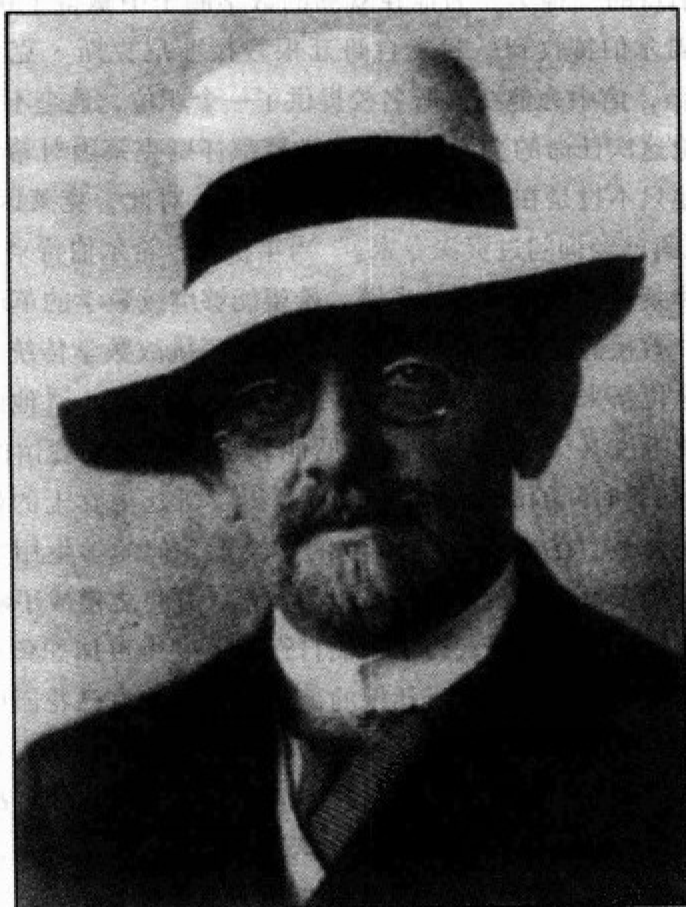


图 23　大卫·希尔伯特，1862～1943

刚涉及这个新开发的领域。到了 19 世纪末期，数论已经枝繁叶茂。为了完成这项任务，希尔伯特邀请自己的老朋友赫曼·闵可夫斯基（Hermann Minkowski）一起工作。在 18 岁时因获得了数学科学大奖而声名鹊起的闵可夫斯基，与希尔伯特在柯尼斯堡求学阶段就已经相识，他很高兴能一起完成这项任务，他认为这是“强大的生命之歌中富有启发性的旋律”。闵可夫斯基断言素数将在他们的关注之下躁动不安，也正是这次合作激起了希尔伯特对素数的兴趣。



希尔伯特的“神学”为他在欧洲的数学圈子中赢得了相当的尊敬。1895年，希尔伯特收到一封发自哥廷根教授菲尼克斯·克莱因（Felix Klein）的信，信中为他在这所名校提供了一个职位，他毫不犹豫地接受了。在讨论这次任命的会议上，许多教授都怀疑克莱因对希尔伯特的支持，认为他只不过是在任命一个自己的亲信。对此，克莱因断然地说，“这个问题我已经询问过资深专家。”当年秋天，希尔伯特来到了这个他的心灵导师黎曼曾担任教授的小镇，希望能够继续数学的革命。

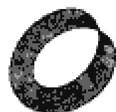
不久，教授们意识到希尔伯特并不满足于挑战数学传统。教授夫人们惊讶于这位新来者的行为，其中一位夫人这样写道，“他颠覆了这里的一切，我听说某天晚上，有人看见他和学生在一家餐馆的后屋打台球。”不过随着时间的流逝，希尔伯特赢得了哥廷根女士的好感，成了著名的花花公子。在希尔伯特50岁的宴会上，他的学生用字母表中的每个数字来代表每位被希尔伯特征服的女士，并将之谱成了歌曲。

108

后来这位风流的教授获得了一辆自行车，变得更加如鱼得水。经常有人看见他骑着自行车穿过哥廷根的街道，带着从自己花园中采摘的花朵去送给情人。由于他经常只穿衬衫讲课，在寒冷的餐馆用餐时，他就会向女食客借来毛围巾御寒。现在并不清楚，是否希尔伯特故意引来争端，或者只是做他认为最简单有效的事。但是可以确定的是，比起社交礼节，他的思想关注数学问题更多一些。

希尔伯特在自己的花园中竖起一块20英尺（6.096米）长的黑板，在照顾花圃和骑自行车之外，他就在黑板上演算数学。希尔伯特热爱聚会，在聚会上他总是选择留声机上最大的针来放出最响的音乐。当他听到卡鲁索①的现场演出时，他十分失望，“卡鲁索用最小的针在演唱。”但是希尔伯特的数学远不像他的个性这样古怪。在1898年时，他的注意力从数论转到几何的挑战上。在19世纪有几位数学家在违反了一条

① Enrico Caruso，恩里科·卡鲁索，1873～1921，意大利歌剧男高音歌唱家，以其有力、纯净和富有感情的声音而被认为是最伟大的歌唱家之一。



希腊人建立的几何基本公理的基础之上，建立了数种新的几何学，这激起了希尔伯特的兴趣，因为他强烈地相信数学的抽象力量，完全不关注任何物理实在。希尔伯特开始研究这几种新几何之下的联系和抽象结构，对他而言只有事物之间的联系才是重要的，他曾表示如果将点、线、面换成桌子、椅子、酒杯，几何理论仍然起作用。

一个世纪之前，高斯就考虑过这些新几何模型带来的挑战，但是他没有公开这些另类的想法。确实希腊人没理由错误，不过他开始质疑欧几里得几何公理中的一条有关平行线的公理。欧几里得曾经考虑过这样的问题：如果画一条直线以及直线外的一点，通过这一点可以作多少条与原直线平行的直线？对欧几里得而言，结果是显然的，有且仅有一条这样的直线。

在 16 岁时，高斯已经怀疑如果不存在这样的平行线，也会有某种相容并且有效的几何存在。除了欧几里得几何，以及这种不存在平行线的几何之外，也许还存在着第三种几何，在这种几何中，存在着多于一条的平行线。希腊人认为，如果存在着这样的几何，那么三角形的内角之和将不再是 180°，而这是不可能的。如果可能存在着数种几何，那么哪一种最能描述真实的物理世界？希腊人相信自己的几何模型是物理世界的数学描述，但是高斯并不完全认同这一点。

在晚年为汉诺威政府服务的岁月中，高斯发明了一种测量方法。利用在三座山顶照出的光线构成的三角形，通过测量三角形的内角和是否为 180°，来判断欧几里得是否正确。高斯认为光线在空间中通过的路径可能是弯曲的，因为三维空间可能会像我们的二维地球表面那样弯曲。高斯的脑中有着大圆的概念，大圆类似于经线，地球上任意两点的最短距离是沿着大圆测量出来的距离。在这样的二维几何中，经线没有平行线，因为它们在极点相交。在此之前，没有人想过或许三维空间也是像这样弯曲的。

现在我们知道，高斯无法观测到任何奇妙的空间弯曲现象来推翻欧几里得的观点，是因为他实验的范围还是太小。1919 年，阿瑟·爱丁顿



(Arthur Eddington) 在一次日食中证实了星光的弯曲，从而支持了高斯的猜测。高斯从未将这些思想公之于众，也许是因为他的新几何看上去与数学的任务——解释物理——实在相去甚远。即使是对朋友，高斯也严守了这个秘密。

18 世纪 30 年代，这些新几何的思想最终被俄国数学家尼古拉·伊万诺维奇·罗巴切夫斯基（Nicolai Ivanovic Lobachevsky）和匈牙利数学家亚诺斯·鲍耶（János Bolyai）公之于众。这些被高斯称为非欧几何的新观念，并没有像高斯害怕的那样破坏数学的现状，仅仅是被认为太过于抽象而被排斥，以至于许多年都无人问津。不过，到了希尔伯特的时代，这些新几何已经逐渐浮出水面，成为数学世界中抽象性的完美体现。

一些数学家断言，如果一种几何不满足欧几里得关于平行线的假设，就会蕴涵某些隐藏的矛盾，从而导致整个体系的崩溃。当希尔伯特开始研究这种可能性时，他发现在非欧几何和欧氏几何之间存在着很强的逻辑联系。如果非欧几何包含着某种矛盾，那么欧氏几何肯定也会含有这种矛盾。这似乎是一种进步。当时的数学家认为欧氏几何是逻辑上完美的音乐，希尔伯特的发现表明这些非欧几何模型具有着同样的逻辑基础。如果一种几何体系崩溃，将导致所有几何体系的崩溃。但是当时的希尔伯特仍怀着不安，因为没有人证明过欧氏几何中不存在矛盾。

110

于是希尔伯特开始考虑如何证明欧氏几何中不包含任何矛盾。虽然自欧几里得以来的 2000 年中，没有人发现过矛盾，但这并不意味着其中没有矛盾。希尔伯特决定首先用公式和方程重建几何学，这项工作首先由笛卡儿提出（因此被称为笛卡儿几何），并被 18 世纪的法国数学家接受。利用描述点和线的方程，几何可以转化为算术，在其中点被转化为描述其空间坐标的数。由于数学家相信数论中不含任何矛盾，因此希尔伯特希望能将几何转化为数，从而可以判断是否欧氏几何包含着矛盾。

然而，抛开需要寻找的结论，希尔伯特发现了更加令人不安的东



西：没有人能真正证明数论本身不含有矛盾。希尔伯特被吓住了。数个世纪以来，无论是在理论还是实验中，数学都毫无瑕疵地正常工作，数学家也对数学有着很强的信心。“Allez en avant, et la foi vous viendra（只要向前，你就会充满信心）”，这是18世纪法国数学家让·勒·让德·达朗贝特（Jean Le Rond d'Alembert）对质疑数学基础的人所说的话。对数学家而言，数的存在就如同生物对于生物学家那样真实。数学家乐于从事自己的职业，从那些不言自明的数的真理出发，用演绎推导出结论，根本没有人会想到这些真理也许会导致矛盾。

希尔伯特被迫越退越远，开始考虑构建数学的根基。既然问题已经提出，就没有办法回避这些最基本的问题。希尔伯特个人相信应该不会发现任何矛盾，这样数学家就能打消怀疑的心理，证明这门学科是建立在坚实基础之上的。希尔伯特的问题标志着数学时代的到来。19世纪已经目睹了数学从作为科学实际需要的女仆转变为对基础真理的理论追求，如同另一位柯尼斯堡的居住者伊曼努尔·康德（Immanuel Kant）的哲学理论一样。希尔伯特对数学最基本的考虑，为他提供了一个平台，使他可以发展他对抽象数学的新实践，而这一实践将在20世纪成为数学的特征。

到了1899年底，希尔伯特被邀请在次年于巴黎召开的国际数学家大会上作大会演讲，这对40岁以下的数学家而言是一个极大的荣耀，同时也给了希尔伯特一个绝佳机会，届时他可以将他对几何、数论和数学逻辑基础的新思想进行整合。

在新世纪到来之际向同行们进行演讲的任务差点使希尔伯特丧失勇气。这是一次真正重要演讲的邀约，同时演讲的内容也应该符合大会的等级。希尔伯特开始向朋友们咨询，是否可以用这次演讲来推测一下数学的未来。这是极不同寻常的想法，并且也违反了数学界的潜规则——只有完整的、成形的思想才能公开发表。需要有极大的勇气才能放弃大会提供的这次用来宣讲已经完成的定理证明的机会，而关注于未来的不可知问题。但是希尔伯特从不惧怕论战，最终他决定用未知代替已知来

111

挑战国际数学联盟。

不过希尔伯特仍有自己的疑惑，利用这样的机会讲述如此超前的内容是否明智？也许他应该遵循传统，讲讲自己证明了什么，而非自己不能解决的问题。由于有这样的疑惑，他错过了提交论文题目的最后期限，因此没有出现在大会的演讲者名单中。到了1900年的夏天，他的朋友都很着急，以为他已完全错过了表达自己想法的最佳机会。但是有一天，他们收到了希尔伯特演讲的内容，题目很简单——“数学问题”。

希尔伯特认为，问题是数学的血液，但是选择问题也要慎重。“数学问题必须足够的难，才能激起我们的兴趣，”他这样写道，“但也不能难到无法下手，免得白白浪费我们的精力。它是我们在迷宫般的道路中寻找真理的路标，是我们最终解决之后幸福的纪念品。”他用严格的标准精心挑选了23个问题，在8月闷热的巴黎大学里，希尔伯特宣讲了他的报告，给新世纪的数学探索者们留下了挑战。

112

19世纪后期，许多学科的研究都受到著名生理学家伊米尔·杜·玻伊斯-雷蒙（Emil du Bois-Raymond）引发的哲学运动思想的影响。他认为人类能力天生有限，无法完全理解大自然。当时哲学圈子里的口号是“Ignoramus et ignorabimus”——我们无知，并且我们将继续无知。但是希尔伯特对新世纪的梦想将这种悲观思想抛到一旁，他用一句鼓舞人心的战斗口号来结束对23个问题的介绍，“每个数学问题都是可解决的！这是我们的信念，也是我们工作的动力。我们心中在不断地呐喊：这里有问题，我要寻找它的答案。你可以利用纯粹的推理找到答案，因为在数学中不存在无知！”

希尔伯特为新世纪数学家提出的问题，正切中了黎曼革命性的思想。希尔伯特问题表中只有前两个问题是他正在考虑的基本问题，其他的问题则涵盖了大部分数学领域。许多问题是开放性的，而非仅仅针对答案的问题。有一条问题与黎曼的梦想有关，就是用数学解决物理中的基本问题。

希尔伯特的第五问题起源于黎曼的观点。黎曼认为数学的不同领



域，如代数、分析、几何等，是密切相关的，我们不能孤立地理解它们；并且黎曼用实例说明了如何从方程的几何图像推导出方程的代数关系。在当时这是勇气的表现，因为经典教条认为代数和分析不应该与具有误导性的几何直观联系在一起，这也正是为什么欧拉和柯西如此反对用图像描述虚数的原因。对他们而言，虚数是像 $x^2 = -1$ 这样的方程的解，而不应该与图像混在一起。但是对黎曼而言，这些学科之间确实存在着联系。

希尔伯特在他的23个问题中也提到了费马大定理。在希尔伯特的时代，这被公认为是数学中著名的未解难题之一，但是它并未能成为单独的一条问题被提出。在希尔伯特的观点里，这只是"科学中非常特殊且看上去很不重要的问题，但是居然产生显著效应的一个典型事例"。高斯也曾表述过类似的观点，因为可以随意选取一些方程，然后问这些方程是否有解。因此费马的选择没有任何特点。

113

希尔伯特选取了高斯对费马大定理的评论作为第十问题的出发点：是否存在一个算法（类似于计算机程序的数学过程），可以在有限时间内判断给定的方程有解？希尔伯特希望他的问题能转移数学家对于特殊方程的关注，并说服他们关注一些更加抽象的东西。比如说，希尔伯特很欣赏高斯和黎曼对素数的新观念，因为数学家不再需要关心某个数是否为素数，而是要寻找那隐藏在所有素数之下的音乐。希尔伯特希望自己的问题也能产生同样的效果。

虽然与会的一位记者描述报告之后的讨论是"一片散漫"，但这更多的是由于8月压抑的天气，而非希尔伯特报告中的呼吁引起。作为希尔伯特最好的朋友，闵可夫斯基说，"全世界的数学家都应该通读这份讲稿，这样你才能吸引更多的年轻数学家。"希尔伯特冒险进行的这次非常规演讲为他赢得了更多的尊敬，他被认为是20世纪新数学的先锋。闵科夫斯基相信这23个问题将产生巨大的影响，他告诉希尔伯特"你为20世纪的数学带来了新生"，事实证明他的话是对的。

在希尔伯特广泛的开放问题表中，第八问题有着特别的意义：证明



黎曼假设。在一次访问中，希尔伯特解释说，他相信黎曼假设是数学中最重要的问题，“而且是绝对重要的问题”。在同一次采访中，当被问道什么是未来最重要的科技成就时，他如此回答，“当然是进行登月飞行。因为要实现它，需要解决众多辅助问题，而这些问题的解决则意味着人类克服了大部分的难题。”如此深刻的见解，描述了 20 世纪的成功之路。

希尔伯特相信，证明黎曼假设对于数学的意义就等同于登月对于科技的意义。将黎曼假设定为自己的第八问题之后，希尔伯特向大会解释道，对黎曼素数个数公式的完全理解，有助于我们理解素数的其他神秘问题，如哥德巴赫猜想和无穷多个孪生素数的存在性问题。证明黎曼假设有两重意义，一方面是结束一段数学历史，另一方面是开启新的数学之门。

希尔伯特没有想到黎曼假设会这么长时间得不到解决。在希尔伯特于 1919 年所作的一次报告中，他乐观地认为能在有生之年看到这个问题被攻克，而在座最年轻的观众将有机会看到费马大定理的解决；同时他大胆地预测，在座的观众将没有人能看到第七问题——判断 2 的$\sqrt{2}$次方是否为某个方程的解——的解决。也许希尔伯特有着很好的数学直觉，但是他的预测能力并不怎么样。不到 10 年，第七问题就被解决。而参加希尔伯特 1919 年报告会的某个年轻研究生也可能有机会目睹 1994 年怀尔斯解决费马大定理。抛开过去数十年间的进展，当希尔伯特像巴巴罗萨一样在 500 年后醒来时，黎曼假设也许仍然没有解决。

曾有一次，希尔伯特认为等待已经结束。某天他收到一位学生寄来的论文，声称解决了黎曼假设。虽然不久希尔伯特在证明中发现了一个漏洞，但是论文中使用的方法令他十分欣赏。不幸的是，这位学生一年之后去世了。希尔伯特被邀请于葬礼上致辞，他称赞了这位学生的想法，并希望有一天能因此找出解决黎曼假设的证明。紧接着他说道，“如果我们考虑这样一个复变函数……”，就这样他完全偏离了演说的主旨，继续讨论起那个错误证明中的细节。这是典型的数学家不通人情世



故的表现，但无论这个故事是否真实，至少它是可信的，有时数学家就是这样。

希尔伯特的报告将黎曼假设推到了聚光灯下，成为了数学中的一道著名未解难题。尽管希尔伯特对黎曼假设如此关注，但是他并没有对这个问题的解决做出任何贡献，不过他为20世纪数学制定的新计划却带来了深远的影响。他关于物理和数学公理化基础的问题，也为19世纪末加深对素数的理解起到了一定的作用。同时，希尔伯特还吸引了另一位数学家来到哥廷根，他将接过从高斯、狄利克雷、黎曼那里传下来的接力棒。

115

朗道：特立独行者

由于希尔伯特的好友，45岁的闵可夫斯基因患上了致命的阑尾炎英年早逝，哥廷根的教职又有了空缺。当时，希尔伯特正成功地解决了华林问题（如何将数写成三次、四次乃至更高次数之和），这个结果正是闵可夫斯基期望的、推广了他18岁那年获得法国科学院数学科学大奖的结果。"即使是在医院的病床上受着病魔的折磨，他仍然关心着下一次讨论班的内容，因为我将在讨论班上报告华林问题的结果，令人遗憾的是，他再也无法出席这次讨论了。"

闵可夫斯基的去世深深地影响了希尔伯特。一位哥廷根的学生说，"有一次课上，希尔伯特谈到了闵可夫斯基的去世，他流泪了。由于当时教授和学生之间的地位悬殊，在课堂上看到他流泪，比听到闵可夫斯基逝世的消息更令我们震惊。"对希尔伯特而言，他急需找到一位继任者，这位继任者对数论的热情应该不亚于闵科夫斯基。

根据大家的意见，希尔伯特挑选的埃德蒙·朗道（Edmund Landau）并不是一个容易相处的人，因此很难决定究竟是选择朗道还是另外一个候选人。希尔伯特问自己的同事，"这两人谁更难相处？"答案不约而同都是朗道。不过希尔伯特认为哥廷根需要朗道，而不需要一个好好先

生。他希望新来的同事不光敢于挑战数学传统，还要敢于挑战社会传统。

朗道对学生非常严格，并且正如传说中一样成为系里的棘手人物。学生经常收到恐怖的周末邀请，在朗道的家里，他们不得不迎合他对于数学游戏的热情。有一次，朗道的一位学生结婚，当出发度蜜月的火车刚要离开哥廷根车站的时候，朗道从天而降，从窗口塞进一叠新书手稿并命令道，“校对完毕，回来交给我!”

不久，朗道作为黎曼和高斯传统的继承人，发展了瓦勒普桑和哈达马的工作，成为欧洲数学界的知名人物。他从瓦勒普桑和哈达马建立的大本营出发，目标直指黎曼假设。为了证明高斯的素数定理，哈达马和瓦勒普桑证明了在穿过 1 的南北向边界上没有零点，下面的任务就是证明在黎曼那条穿过 1/2 的临界线右方也没有零点。

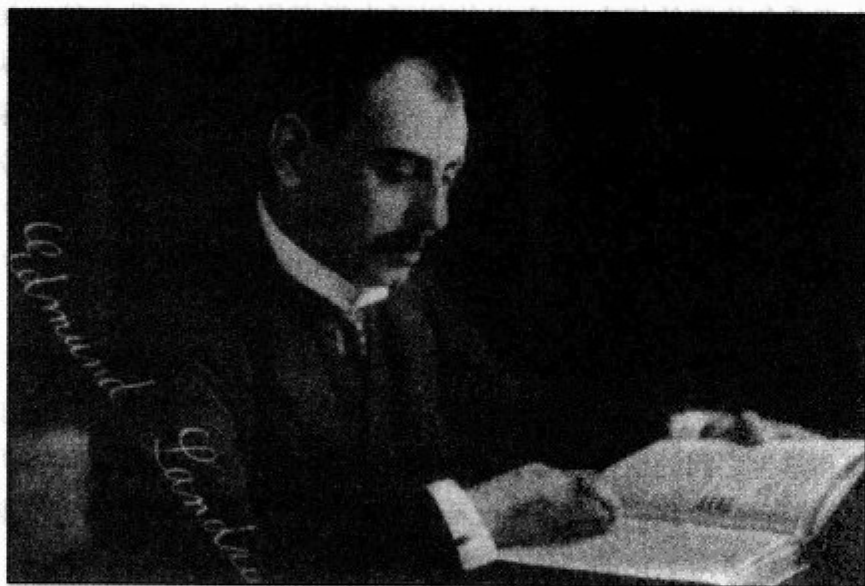


图 24　埃德蒙·朗道，1877 ~ 1938

这时，哈拉德·玻尔（Harald Bohr）加入了朗道的工作。玻尔在哥本哈根工作，同许多数学朝圣者一样，他穿越欧洲来到哥廷根。玻尔的



兄弟，尼尔斯·玻尔（Niels Bohr）后来因为建立量子理论而成名。同时，玻尔还作为丹麦足球队的主力获得了1908年奥运会的银牌。

朗道和玻尔一起对黎曼平面上位于海平面的点发动了一次成功的攻击，并证明了大部分零点都聚集在黎曼的临界线附近。他们考虑了从0.5到0.51之间的零点个数，并与在此范围之外的零点数相比较，他们能证明在此条状区域内的零点占所有零点的绝大部分。黎曼猜测所有的零点都落在穿过1/2的那条临界线上，虽然朗道和玻尔没能证明这一点，但至少他们开了个好头。

117

实际上，条状区域的宽度并不需要限制为0.01，无论多么窄，即使是$1/10^{30}$那样，朗道和玻尔仍旧可以证明大部分的零点都位于这样的条状区域中。令人遗憾的是，朗道和玻尔无法说明这样就意味着大部分零点都位于穿过1/2的临界线上。黎曼曾宣称自己已经证明了该结果，但是没有发表。朗道和玻尔的结果与直觉是矛盾的，如果所有的零点都位于一个不断缩小的条状区域中，为什么就不能说明它们中的大部分就是落在临界线上？这就是数学的神秘所在，我们假设对每个数N，都有10^N个零点位于条状区域$1/2+1/10^{N+1}$和$1/2+1/10^N$之间，这就满足了朗道和玻尔的结果，但是却没有一个零点落在黎曼那条穿过1/2的临界线之上。

当时的哥廷根，就如同镌刻在市政厅上的格言宣称的那样，在中世纪的城墙之外没有生活。但是由于希尔伯特的影响，这个安静的大学城在20世纪前期成为了世界数学中心。黎曼在世时，柏林大学是知识分子云集的地方。后来当希尔伯特收到柏林大学的邀请时，他拒绝了，因为承继着高斯传统的这个中世纪小镇是进行数学研究的最佳之地。

希尔伯特能将世界上最好的数学家吸引到哥廷根，多亏了一位数学教授的慷慨捐赠。1908年去世的保罗·沃尔夫斯凯尔（Paul Wolfskehl）在遗嘱中留下了10万马克，用于奖励第一个证明费马大定理的人。怀尔斯在童年时期就听说过这个奖，并因此被激发了挑战费马谜题的愿望。（怀尔斯最终因为证明了费马大定理得到的奖金，由于两次世界大



战之后的恶性通货膨胀而大大缩水。）沃尔夫斯凯尔的遗嘱中规定，如果当年无人能证明费马大定理，那么奖金的利息将用来资助那些来哥廷根的访问学者。

118

当时，朗道负责检查那些寄往哥廷根的解答。很快朗道就没有足够精力处理如此多的解答，于是他将这些手稿交给学生，并附上一些标准的回信，学生只需在空白的地方填空即可。信上如此写道，“谢谢您寄来的关于费马大定理的证明，第一个错误出现在第____页第____行。”另一方面，希尔伯特则轻松得多。他负责处理这笔奖金的利息，因此他可以灵活地利用这笔钱吸引数学家来到哥廷根，并且这笔钱的数量可观。因此希尔伯特甚至希望费马大定理永远无法得到解决，“为什么我要杀死一只会下金蛋的鹅呢？”

许多年轻的数学家要想成为世界知名的人物，往往第一步就是去哥廷根。一位学生如此形容希尔伯特在数学界的影响，“他就像吹着魔笛的笛手……我们这些鼠辈被他优美的旋律吸引，跟着他一步一步踏入数学的河流。”事实也确实如此，哥廷根吸引了来自欧洲大陆的许多青年数学人才。他们原先就读于那些在19世纪欧洲的政治和知识革命中诞生的学院，现在则纷纷来到哥廷根。

相比较而言，英国受传统之累，一时不能吸收来自欧洲大陆的新思想。英国的海岸不光成功抵抗住了来自法国大革命的政治影响，同样也将黎曼的数学革命拒之门外。虚数被认为是欧洲大陆的危险记号。实际上，自从17世纪牛顿和莱布尼兹关于微积分的发现权之争开始，英国的数学就没有了曾经的辉煌。即使牛顿是第一位，但是拒绝承认莱布尼兹在该学科的优势，英国数学也无法全面发展。然而到了近代，事情终于有了转机。

哈代：数学唯美主义者

到了1914年，朗道和玻尔已经成功证明，绝大多数的零点集结于



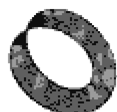
黎曼临界线的附近。但是确定究竟有多少点落在临界线上，数学家还有很长的路要走。到当时为止，在无穷多位于海平面的点中，数学家仅仅能确定有 71 个点是落在临界线上，

经过了两个多世纪对欧洲大陆思想的漠不关心，英国数学界终于从思想上出现了重大突破。英国数学家哈代接过了黎曼的接力棒，证明了有无穷多个零点确实是落在这条穿过 1/2 的南北向临界线上。哈代的贡献给希尔伯特留下了深刻印象。后来，当希尔伯特发现哈代在剑桥三一学院碰到住宿问题的时候，他特别写信给学院的负责人，称哈代不光是三一学院最好的数学家，也是英国最好的数学家，理应得到学院最好的住房待遇。

哈代在数学界之外的声名，很大程度上来自于他那篇文辞优美的自传《一个数学家的自白》；在数学界之内，他则因素数理论和黎曼假设而知名。哈代证明了有无穷多个零点落在临界线上，是否说明游戏已经结束？哈代是否证明了黎曼假设？如果已知存在无穷多个零点，并且哈代已经证明了其中有无穷多个落在黎曼的临界线上，是否这就代表着大功告成？

然而，无穷的性质不可捉摸。希尔伯特喜欢用一个旅馆的例子来描述无穷的神秘性：这个旅馆有无穷多间房间，如果所有的奇数号房间都已经预定出去，虽然这样的奇数号房间有无穷多，但是仍然有无穷多间偶数号的房间可供预定。在哈代的问题中，房间的预定情况就相当于判断零点是否落在临界线上。可惜的是，即使是证明至少有一半的零点落在临界线上，哈代也无法做到。对哈代而言，他已经预定了无穷多个房间，但是这无穷多个房间相对于所有可供预定的房间而言，只有百分之零。哈代的成就是显著的，但是剩下的路途依然漫长。哈代已经确定了一部分零点的位置，但是剩下的部分仍然和以前一样多，也一样难。

对哈代而言，这次尝试如同初尝毒品。从此，除了对板球的热爱以及与上帝的交战，证明所有的零点位于临界线上就占据了哈代所有的时间。和希尔伯特一样，黎曼假设也成为哈代希望攻克的难题的第一位，



这也可以从他寄给朋友和同事的明信片上的新年愿望中看出：

(1) 证明黎曼假设。

(2) Oval 体育场举行的国际板球锦标赛决赛第四局不会出现 211（200 分之后的第一个素数）。

(3) 找出一个可以令公众信服的、证明上帝不存在的论述。

(4) 成为攀登珠峰第一人。

(5) 被宣布成为英国和德国第一位苏维埃社会主义共和国联盟总统

(6) 谋杀墨索里尼。

哈代很早就被素数吸引。在孩童时期，他就乐于在教堂中将圣歌中的数分解为素数因子。他喜欢阅读关于这些基本数的奇异性质的书，他认为这些书“比清晨早餐桌上的足球报道更有趣”。实际上，哈代认为喜欢看足球报道的人也应该能欣赏素数的乐趣，“这是一种特殊的关于数的理论，大部分内容都易懂，并且能为《每日邮报》吸引一批新的读者。”哈代相信素数中包含了大量的吸引读者的神秘之处，并且简单到任何人都可以进行一些探索。和同时期的数学家不同，哈代尽可能地展示他对这门学科的热爱，他认为素数理论不应该是学院派象牙塔中的私密娱乐。

从哈代新年计划中的第三点也可以看出，教堂对他的影响同样很深。很早的时候，哈代就成为了上帝存在和宗教信仰的坚决反对者。他毕生从事着反对上帝的战争，试图证明上帝的不存在。哈代与上帝的斗争具有强烈的个人色彩，他想象着某个角色，但是又强烈地否认这个角色的存在。在他去看板球比赛的时候，哈代总是带上自己的一套反上帝的装备来避免下雨。即使天空万里无云，他也要带上四件毛衣、一把伞和一堆书籍。面对体育场邻座的观众，他解释说这一切都是为了戏弄上帝，让上帝误以为他希望能在下雨的时候阅读书籍。哈代认为上帝——他自己的敌人——会为了阻止他进行数学研究而艳阳高照。

在某一场夏天的板球比赛中，因为击球手抱怨说看台上总是发出的



阵阵闪光影响了他的正常视力，导致比赛不得不突然中断。哈代对此非常失望，不过很快看台上的一位牧师就被要求摘下脖子上巨大的十字架，因为十字架是反射阳光的罪魁祸首。哈代顿时由悲转喜，并趁着午休时间，给自己的朋友们寄出了一系列的明信片，描述这件板球战胜神父的趣事。

当每年的板球赛季于9月份结束之后，哈代总可以在英国大学新学期开学之前的一段时间里去拜访哥本哈根的玻尔。他们每天的工作很程式化：早晨放一张纸在桌子上，哈代在上面写下今天将要完成的工作内容——证明黎曼猜想。哈代乐观地认为，玻尔在哥廷根发展的思想将为证明提供新的思路，但是他们迎来的却是一次次的失败。

有一次，因为新学期的到来哈代不得不返回英国。在他离开哥本哈根后不久，玻尔收到了一张明信片。信上的句子让玻尔目瞪口呆，“已经得到了黎曼假设的证明，由于明信片太小而无法写下。”看上去最终还是哈代完成了这个任务。但是玻尔心里明白，明信片上的话十分类似费马在书页空白处留下的评论，是哈代故意开玩笑在明信片上留下这样的话吗？玻尔决定暂不透漏这个消息，以等待哈代更多的细节。最后事实说明，玻尔期望的那个结果并没有出现，这个明信片只是哈代与上帝开的又一个玩笑。

从丹麦回英国的轮船需要穿越北海，当哈代上船时，海面上波涛汹涌。由于船并不大，哈代很担心自己的安危。但是他有自己特殊的保险策略，那就是他寄给玻尔的明信片，上面记载着他杜撰的发现。哈代一生中最重要的事情就是证明黎曼假设，其次则是与上帝的战争。哈代知道上帝不会让船沉没，因为那样，世人就会传说哈代与黎曼假设的证明一起葬身海底。哈代的策略成功了，他安全地返回了英国。

可以毫不过分地说，正是哈代对黎曼假设的热情，加上他本人传奇色彩的个性，让黎曼假设登上了数学难题的首位。哈代在《一个数学家的自白》中优美如诗的语言，极大地提高了数论以及许多问题的重要性。哈代在《一个数学家的自白》中所有关于数学美的言论同样令人印



象深刻，然而在许多情况下，哈代所推崇的证明的优美性往往不是那么明显，它们会被众多必要的技术细节掩盖。通常，成功大多是来自于思想的灵活运用，而非思想本身。

吸引哈代成为数学家的那一本书根本就不是数学书。那是一本描述三一学院生活的小说，小说《三一学院成员》中描写的在教师公用教室中的饮水装置吸引了哈代。哈代承认他选择数学是因为“这是我唯一可以做好的事……如果我可以做到，数学就意味着能为我在三一学院谋得职位。”

122

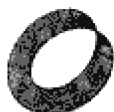
为了得到这个职位，哈代经受了剑桥大学规定的重重考试的考验。后来哈代明白，考试中涉及的人工技术和数学智力问题意味着，即使你已经完成数学学位的学习，也不代表你清楚数学究竟是干什么的。1904年，哥廷根的一位教授仿造英国的试题出了这样一个题目：“在弹性的桥上站着一头大象，大象的重量可以忽略不计，大象鼻子上有一只质量为 m 的蚊子，当大象甩动鼻子进行圆周运动时，计算桥梁的振动。”考试将牛顿的《原理》看作是圣经，希望同学在考试中能正确引用；考试看重的更多是结果，而无论这些结果在实际中意味着什么。哈代认为正是这样的教育体系造成了英国数学长时间的荒芜。英国的数学家被训练得可以迅速地演奏出单个数学音符，而不清楚一旦他们掌握了这些数学音符之后，将会奏出多么美妙的音乐。

哈代认为自己的数学启蒙书籍是法国数学家卡米勒·若当（Camille Jordan）的《分析教程》（Cours d'Analyse）。这本书帮助哈代认识了欧洲大陆的数学，“我永远无法忘记首次读到这本名著时的震惊……并且首次认识到数学真正的含义。”

1900年，哈代被选为三一学院的成员，从考试的义务中解脱出来，可以自由地在真实数学世界中探索。

利特伍德：数学牛仔

1910年，一位比哈代年轻8岁的数学家来到三一学院，加入了哈代



的研究。利特伍德（J. E. Littlewood）与哈代一起合作了37年。他们像是数学中的斯科特和奥茨[①]，探索着欧洲大陆已经开发的数学新领地，合作的论文超过了100篇。玻尔经常开玩笑地说，当时英国有三位最著名的数学家：哈代、利特伍德以及哈代-利特伍德。

两位数学家将各自的优势带到了合作之中。利特伍德是牛仔型的学者，他全副武装地解决问题，并着迷于征服难题带来的满足感；与之相反，哈代推崇数学中的优美与简练。这一性格也延续到他们合作的论文写作中，哈代一拿到利特伍德粗糙的手稿，就会加入他们所谓的“气体”语句，使得论文中的证明总是伴随着优美的散文语句。 123

奇怪的是，这两位数学家的风格也反映在他们各自的外形上。哈代长得很英俊，属于那种驻颜有术的人。在三一学院的早年岁月中，他常常被教师公用教室中的其他同事怀疑是因为三一学院迷宫般的走廊而走错教室的本科生。利特伍德则不修边幅——“就像是狄更斯笔下的角色”，一位数学家这样描述利特伍德。他的思想和身体一样强壮并且灵活，他和哈代一样热爱板球，是一位强有力的击球手。利特伍德另一样爱好是音乐，这是哈代永远也不可能涉及的领域。利特伍德自学钢琴，并且对巴赫、贝多芬和莫扎特的音乐有着强烈的热爱，他认为生命太短暂，没有必要浪费时间在那些不重要的作曲家身上。 124

他们两人在性取向方面也存在着差异，众所周知哈代有很大可能是同性恋。在当年的牛津大学和剑桥大学，如果教师结婚，将会失去他们的教职。因此在剑桥的校园中承认同性恋比婚姻更容易，但是哈代对此依然很谨慎。利特伍德则称哈代是一位“名不副实的同性恋者”。据大家的传说，利特伍德是一位讨女性欢喜的男人，当然在这方面还比不上

---

① Scott and Oates，英国的两位著名探险家。1912年，罗伯特·福尔肯·斯科特（Robert Falcon Scott）率领包括劳伦斯·奥茨（Lawrence Oates）在内的5人南极探险队到达南极极点。然而在一个多月前，挪威人阿蒙森已经率先抵达极点，成为首位到达南极极点的人。在回程中，五人相继因饥饿与暴风雪而去世。现在位于南极极点的科考站被命名为阿蒙森-斯科特站。





图 25　哈代和利特伍德在剑桥三一学院，1924 年

希尔伯特。利特伍德曾与一位当地医生的妻子关系密切，每年一起在康沃尔郡度过暑假。许多年之后，这位女士的一个孩子看着镜子中的自己，说自己很像约翰叔叔，女士马上说道，“这并不奇怪，因为他就是你的父亲。”

作为完美的搭配，哈代和利特伍德的合作基于如下具体原则：

> 规则一：无论他们写给对方的信是否正确，都不重要。
> 规则二：没有强制性的阅读并回复对方来信的要求。



规则三：两人尽量不要同时考虑相同的问题。

最重要的公理则是：

规则四：为避免争吵，所有的论文都由两人共同署名，即使某人对此毫无贡献。

玻尔如此总结他们两人的关系："从来没有人基于像这样消极的规则，完成了如此重要并且融洽的合作。"今天的数学家在涉及合作的时候仍然会谈论到"哈代-利特伍德规则"。玻尔发现，即使在哥本哈根与自己合作时，哈代仍然遵循着合作规则。玻尔记得每天都有很多利特伍德写来的数学信件，哈代平静地将它们扔到一边，轻描淡写地说："我想等我有空再读这些信。"当哈代在哥本哈根时，只有一件事铭记在心：黎曼假设。除非利特伍德寄来一份黎曼假设的证明，否则利特伍德来信的归宿仍然是墙角。

利特伍德的学生哈罗德·达文波特（Harold Davenport）曾经说过一件事：哈代与利特伍德曾经因为黎曼假设而闹翻。哈代写过一篇凶杀推理小说，在其中一位数学家证明了黎曼假设，不料另一位数学家将他谋杀，并宣称是自己证明了黎曼假设。利特伍德很伤心，原因并非因为哈代没有遵循规则四，将他列为共同作者；而是利特伍德认为其中的杀人者是以自己为原型。因此他反对将手稿进行发表，最后哈代作出了让步，这颗文学的明珠最终没有出现在数学的世界中。

利特伍德是剑桥本科生中的杰出学生，他能应付各种形式的考试。经过重重选拔，利特伍德成为顶尖的学生，成为人人嫉妒的数学学位甲等获得者，同时获得这个称号的还有另外一位学生梅瑟（Mercer）。数学学位甲等获得者是剑桥中的名人，他们的照片会在学期末出售。也许当年利特伍德的同学们已经预感到这个人将来会很有出息，因此当利特伍德的一位朋友试图去购买照片时，他被告知"利特伍德先生的照片已经售空，但是梅瑟先生的照片还有不少。"



利特伍德明白学校中的考试，并不能说明数学的功用，而仅仅是一些技术游戏。但是这些游戏必须掌握并且获胜，否则就不能进行更高层次的学习。“这些游戏对我而言很容易，有时我甚至对自己的能力感到满意。”利特伍德希望能将这些从本科阶段学习到的技巧应用到更加具有创造力的工作中去，但是利特伍德即将面对的严肃数学研究，对他无疑是一次严峻考验。

抛开了考试，利特伍德渴望在暑期长假中能进行研究工作。他询问了自己的导师欧内斯特·巴内斯（Ernest Barnes），希望他能为自己选择一个恰当的问题，来试试自己的能力。后来成为伯明翰主教的巴内斯想了想，想起了一个有趣的函数。这个函数在当时还没有人能真正掌握，也许利特伍德可以找出这个函数的零点。巴内斯写出了这个函数的定义，并将它交给利特伍德，“这是 ζ 函数”，巴内斯平静地说。利特伍德拿着这张纸，走出了巴内斯的屋子，并没有在意巴内斯刚刚建议的、让他在暑期试着证明的黎曼假设。

126

巴内斯的失误是没有告诉利特伍德这个问题的历史背景，那意味着这个问题的难度。作为利特伍德的导师，他并没有意识到零点与素数之间的联系，只是将它认为是一个孤立的趣题：这个函数的零点在哪里？现代黎曼假设的前线人物之一彼得·萨那克（Peter Sarnak）说，“进入20世纪，这仍然是唯一的尚未完全理解的分析函数。”利特伍德的学生，斯文那顿-戴尔爵士（Sir Peter Swinnerton-Dyer）在利特伍德的追悼会上回忆说，“巴内斯认为（黎曼假设）适合于最聪明的学生，而利特伍德就是这样的学生”这一事实，说明了在哈代和利特伍德产生深远影响之前，英国数学界的可怕现状。

利特伍德奋战了整个暑假，试图征服巴内斯给他的看上去很简单的函数。尽管他没有找出零点的分布，但是却得到了某些意想不到的结果。正如黎曼在50年之前发现的，利特伍德意识到这些零点隐含着某些素数的性质。对于欧洲大陆的数学界，这一点已是公认的结果，但是英国数学家对 ζ 函数与素数之间的这一联系还一无所知。利特伍德对自



己的新发现感到很兴奋，他于1907年9月将它写成论文，用来申请三一学院的教职。利特伍德认为自己的发现是全新的，这也进一步说明当时的英国数学界是多么的孤立。

作为英国少有的、对哈达马和瓦勒普桑的成果有所耳闻的数学家，哈代知道这个结果并不像利特伍德认为的那样是全新的发现，但是哈代却因此看到了利特伍德的潜力。那一年利特伍德并没能获得三一学院的教职，但是却有一个君子协定同意他在下一轮入选，于是在1910年的10月，利特伍德终于成为三一学院的成员，成为了哈代的同事。

当剑桥敞开大门，接受那些穿越英吉利海峡的智力传统的影响之后，它获得了蓬勃的发展。英国与欧洲大陆之间的交往更加容易，哈代与其他学者纷纷拜访欧洲的学术中心，这些交流带来了国外新的杂志、书籍和思想。在20世纪的早期，三一学院更是成为了活跃的中心。教师公用教室不再是绅士的俱乐部，而是成为了研究的场所。贵宾桌上的交谈不再限于酒类，而是充满当天的新思想。同样是在三一学院，除了哈代和利特伍德，还有英国最著名的两位哲学家：伯特兰·罗素（Bertrand Russell）和路德维格·维特根斯坦（Ludwig Wittgenstein），他们与希尔伯特一样，研究着数学的基础问题。此时的剑桥产生了许多物理学上的突破，像汤姆逊①（J. J. Thomson）因为发现电子获得诺贝尔奖，爱丁顿发现空间是弯曲的并且是非欧的，从而证实了高斯和爱因斯坦的推断。

从哥廷根传来的一本朗道关于素数的书籍，激发了哈代和利特伍德之间最伟大的合作。这本出版于1909年、上下两卷的《素数理论与分布手册》（*Handbuch der Lehre von der Verteilung der Primzahlen*）记录了素数与黎曼ζ函数之间的奇妙联系。在这本书出版之前，黎曼的素数故事在数学界中只是小范围的流传。在哈代为朗道写的讣词（与Hans Hei-

---

① 全名Joseph John Thomson，1856～1940。英国物理学家，电子的发现者，并因此获得1906年诺贝尔物理学奖。



lbronn 合作）中，他感谢道，“这本书的出现让一门仅有数位探索者的学科，转变为近 30 年来最热门的学科之一。”哈代正是在朗道的这本书的激励之下，于 1914 年证明了有无穷多个零点落在黎曼的临界线上。而由于学生时代对 ζ 函数的研究，利特伍德也被激发起了兴趣，并做出了在该领域的首个重要成果。

高斯认为正确但他自己不能证明的定理，被公认为是对数学家勇气的真正挑战。而试图推翻这些定理的人，则被认为是脑袋有问题，因为高斯的直觉极少出错。高斯提出的对数积分函数 Li（N），可以预测直到 N 的素数个数，并且当 N 增大时，这个函数的精确度不断提高。哈达马和瓦勒普桑证明了高斯直觉的正确性，从而让自己留名青史。然而高斯还做出了第二个猜测：函数 Li（N）对素数个数的估计总是过多——这意味着从 1 到 N，这个函数估计出的素数个数，永远要比真实的素数个数多。但是这个猜测与黎曼的改进相矛盾，因为相对于真实素数个数，黎曼的改进总是在过多与过少之间波动。

128

当利特伍德开始考虑高斯的第二个猜测时，这个猜测已经被验证对 10 000 000 以内的数都正确。任何实验型科学家有了 1000 万的实例证明之后，都会完全支持高斯的直觉。看重实验结果的学科很容易就会接受高斯的猜测，并将它作为已知结果，在其上建立新的理论。如果是那样，到了数百年之后的利特伍德时代，在此基础之上早就已经建立了高耸入云的数学高塔了。但是在 1912 年，利特伍德发现，与人们的期望相反，高斯的猜测只是海市蜃楼。经过利特伍德的仔细审查之后，这块期望中的数学基石崩溃为一堆尘土。利特伍德证明了，只要 N 足够大，总会存在一个区域，在此区域高斯的估计将从过多变为过少。

利特伍德还成功地推翻了先前被广泛承认的一个观点，就是黎曼的改进公式比高斯的素数个数公式要更加精确。利特伍德证明了，在前 100 万个数之内，黎曼的公式确实要比高斯的公式精确，但是当你继续考虑更多的数时，高斯的公式有时能给出比黎曼公式更准确的估计。

关于利特伍德的发现，奇妙之处还在于，尽管我们知道高斯的素数



个数公式会在某一区域过少估计素数的个数，但是这一区域我们也许永远也无法达到。即使是利特伍德也说不清楚究竟数到多少时，我们可以观测到这一现象。实际上，直到今天我们也没有达到这样的一个区域，高斯公式在其中会过少估计素数的个数。正是利特伍德的理论分析以及数学证明的力量，才使得我们如此确信，确实存在这么一个区域，在其中可以推翻高斯原先的猜测。

数年之后的 1933 年，利特伍德的一位研究生斯坦利·斯库斯（Stanley Skewes）计算出，如果你能数到 $10^{10^{10^{34}}}$，那么你将看到高斯的素数公式结果比真实的素数个数要少。这是一个奇大无比的数，一般人们碰到大数时，会将它和整个可见宇宙中的原子数相比。宇宙中原子数最好的估计是 10^{78}，但是斯库斯提出的这个数还要大出许多。即使你在 1 的后面写上宇宙中的原子数个零，也就是 10^{78} 个零，还是要远远小于这个数。哈代将这个数称为斯库斯数，现在我们知道，这肯定是所有数学证明中出现过的最大的数。

129

斯库斯的证明之所以有趣，还存在着另外一个原因，这个证明是基于“黎曼假设正确”前提之下数以千计的证明之一。只有在黎曼假设正确的前提之下，即 ζ 函数所有位于海平面的点都落在穿过 1/2 的临界线上，斯库斯的估计才是正确的。如果没有这个前提，19 世纪 30 年代的数学家将无法估计出究竟需要多远，我们才可以观察到高斯的猜测少于真实素数个数的情况。在这个问题上，数学家最终找到了一条无须翻越黎曼峰的道路。1955 年，斯库斯找到了一个更大的数，这次，即使黎曼假设是错误的，我们也可以观测到期望中的结果。

奇怪的是，数学家不太愿意相信高斯的第二猜测，但却对黎曼假设的正确性抱有强烈的信心，并且愿意在此之上发展新的理论，而不管它是否正确。现在黎曼假设已经成为数学大厦中的必要部分，但是它的实用性和它的正确性一样成问题。越来越多的数学家发现在数学的道路上经常会碰到黎曼假设，并且只有承认它的正确性才能继续前行。但是正如利特伍德推翻的高斯第二猜测一样，只要有人发现存在某个零点，它



落在临界线之外，等待着数学家的不光是黎曼假设被推翻，而且在此基础之上建立的所有理论也将全部崩溃。

利特伍德的证明对数学家的直觉产生了深远的影响，特别是对素数的判断。它对于那些易被大量数值证据影响的数学家，是一个严厉的警告。它揭露了这样的事实：素数是伪装大师，它们将自己的本质深深隐藏于数的宇宙之中。它们藏得如此之深，人类的计算能力根本不足以窥探它们的真实本性，只有抽象的数学证明的锐眼才能看穿它们的真实行为。

利特伍德的证明还为那些关于数学在本质上是否与其他学科不同的论战提供了强有力的弹药。从此，数学家无须再接受从 17、18 世纪以来数学被打上的实验主义的标签，基于少量的计算提出理论的经验主义不再是指引数学世界发展方向的合适媒介。对于其他学科而言，数百万条证据已经足够，但是利特伍德证明了，即使这样，在数学中我们仍然如履薄冰。从此以后，证明就是一切，如果没有决定性的证据，什么也不能相信。

130

当越来越多的数学家被迫假设黎曼假设的正确性时，证明没有零点位于临界线之外变得比以往更加迫切。除非这一切完成，否则数学家将永远生活在恐惧之中，害怕黎曼假设在某一天被推翻。

131



第六章

拉马努扬，谜一般的数学家

对我而言，只有体现神的意志的公式才有意义。

——斯尼瓦萨·拉马努扬

当哈代和利特伍德在黎曼的奇妙世界中披荆斩棘时，远在8000千米之外的印度马德拉斯港政府办公室中，一位名叫斯尼瓦萨·拉马努扬（Srinivasa Ramanujan）的办事员正被素数种种神秘的、令人兴奋的变化所吸引。他抛开那些本来应该做的工作，花费整天整天的时间来观察和计算，搜寻素数中奇妙性质的原因所在。当拉马努扬计算素数时，他根本不知道西方已经发展出来的复杂观点，并且他本人没有受过任何正规的教育，根本不可能像哈代和利特伍德那样对数论这门学科，甚至是素数怀着深深的敬意，认为这是"纯粹数学所有分支中最困难的"部分。由于没有受到任何数学传统的约束，拉马努扬完全以纯粹的热情投入到素数的研究中。他这种发自天性的行为，加上他超常的数学天赋，最终成为了他的优势。

在剑桥，哈代和利特伍德沉醉在朗道关于素数的著作带来的奇妙世界中。在印度，拉马努扬对素数的兴趣则来自于一本更基础、但是影响深远的书。对于年轻的科学家而言，在他们的生命中总有着对未来起着关键作用的转折点。比如说黎曼，正是他在少年时得到的勒让德的著作在他心中种下种子，并在后来的日子中生根发芽；对哈代和利特伍德而言，朗道的著作有着同样的作用。15岁的拉马努扬则在1903年得到了一本乔治·卡尔（George Carr）的《纯粹与应用数学中的基础结果概



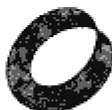
要》(*A Synopsis of Elementary Results in Pure and Applied Mathematics*)。除了与拉马努扬的联系，这本书及其作者都没有什么名气，但是书的结构却很有意思，其中列举了大概4400个经典的结果——仅仅是结果而没有任何证明。拉马努扬花费数年时间通读了本书，并将其中的结果一一验证。由于不熟悉西方风格的证明，拉马努扬被迫创造了自己的数学语言。缺少了正规教育接受模式的束缚，拉马努扬可以在数学的世界中自由徜徉，不久他的笔记本中就记满了远远超出卡尔书中结果的新思想和结论。

132



图26 斯尼瓦萨·拉马努扬，1887～1920

欧拉曾经通过解决许多费马留下的未证明论断小试牛刀，同样在拉马努扬解决问题的方法中可以找到欧拉的影子。拉马努扬有种奇妙的直



觉，他知道如何通过这样或那样的公式变换得到对问题的新理解。当他单独发现虚数在指数函数和波动方程之间的联系时，他非常兴奋，但是数天后，他发现欧拉早在150年之前就已经做出了这个伟大的发现，快乐转变为失望。受此挫折，拉马努扬将自己的计算过程藏到了屋顶之中。

即使给予充足的时间，数学家的创造力也是难以理解，而拉马努扬思考的方式更是一个谜。他常常声称自己的思想是来自于梦中女神Namagiri，她是毗湿奴[①]召唤出的狮面神Narasimha的妻子，也是拉马努扬家族的守护神。拉马努扬村子里的其他人相信女神可以驱除妖孽，而拉马努扬本人认为，她是自己源源不断作出数学发现的思想灵感之源。

将梦中世界看作是数学探索灵感来源的数学家，并非只有拉马努扬一个。狄利克雷曾经在晚上将高斯的《算术探讨》放在枕头下面，希望能够得到灵感，理解这本书中的隐讳话语。也许他们认为，在晚上思想可以脱离真实自然界的约束，自由地探索那些白天无法触及的领域。而拉马努扬似乎可以在白天也拥有这种梦中状态，这种沉迷的状态也是许多数学家试图接近的思想状态。

因为证明素数定理而成名的哈达玛，着迷于数学家的创造性思维的原因，他将自己的思想归结于1945年出版的《数学发明的心理学》(*The Psychology of Invention in the Mathematical Field*)，在其中哈达玛强调了潜意识的重要性。现在神经学家也对数学思维的运转方式产生了越来越多的兴趣，因为从中可以探察大脑活动的细节。在休息或在梦中，思想可以自由地徜徉于那些白天吸收进来的知识之中。

在这本书中，哈达玛将数学发现的行为分成四个阶段：准备阶段、沉思阶段、激发阶段和证实阶段。如果说拉马努扬具有第三阶段的天

---

① 印度主要神灵之一，作为世界的保护和维持者受到崇拜。毗湿奴常被认为是包括大梵天和湿婆在内的三位主神中的一员。



赋，那么他明显缺乏第四阶段的能力。不过对他而言，激发阶段就已经足够了，他只是不明白证实阶段的关键所在。也许，没有了证明的约束，拉马努扬能够更加自由地在数学的荒野中找到新的道路。这种直觉性的风格与西方的科学传统明显格格不入，利特伍德后来写道，"他完全不能理解证明中体现出来的清晰思想，如果事实与直觉给了他足够的把握，他就不再向前看了。"

印度学校基本上继承了大英帝国的制度。然而，英国的教育系统培养了利特伍德和哈代，却不能在印度正确地培养拉马努扬。1907 年，当利特伍德的论文被剑桥大学接受时，拉马努扬没有通过大学的入学考试，这是他第三次也是最后一次尝试。如果入学考试只有数学，拉马努扬一定可以通过，不过他需要准备的还有英语、历史、梵文和生理学。作为一名保守的婆罗门，拉马努扬是严格的素食主义者，因此解剖青蛙和兔子对他而言是不可能的。但是拉马努扬的失败，也就是无法进入马德拉斯大学，并没有扑灭他心中的数学之火。

134

到了 1910 年，拉马努扬渴望自己的思想得到承认。特别的是，他很得意于自己发现了一个公式，能够很精确地计算出素数个数。起初，他与大多数人一样，对无法驯服这些数感到灰心丧气。但是拉马努扬知道素数对数学而言是如此的基础，因此他没有放弃，坚信一定存在某个数学公式能够解释它们。他天真地认为所有的数学与规律都可以准确地用方程和公式表示。利特伍德后来这样说道，"如果拉马努扬早出生 100 或 150 年，那他将是一位伟大的数学家。要是恰好和欧拉处于同一时期，又会出现怎样的景象？……但是公式的时代已经过去了。"19 世纪与 20 世纪的交界是数学的转变之际，但是拉马努扬并非为此而生，他的目标是发现素数的公式。经过长时间的研究素数表，他发现了一个规律，并且他渴望将这个发现告诉能够欣赏它的人。

拉马努扬清晰的笔记，以及婆罗门圈子的人际关系，为他谋得了马德拉斯港口办公室的一份职位。不久他开始在《印度数学学会学报》上发表自己的一些观点，并引起了一位英国官员葛瑞夫（C. L. T. Griff-



th）的注意。葛瑞夫在马德拉斯工程学院工作，他意识到拉马努扬的结果可以与那些“杰出数学家”的结果相比较，只是他本人无法理解，因此他决定征询伦敦一位教授的意见。

由于缺少正规的训练，拉马努扬发展出一套自己的数学风格，他在自己的论文中宣称证明了

$$1+2+3+\cdots+\infty=-\frac{1}{12}$$

这个结果。因此一点也不奇怪，当伦敦大学的希尔（M. J. M. Hill）教授看到这个公式时，理所当然地认为其余内容都是无意义的。因为即使是一个未经训练的人，也可以看出这个公式是荒谬的。将所有的数相加，最后竟然得到一个负分数，得到这个结果的人一定是疯子！“拉马努扬先生落入了极难的发散级数的陷阱之中。”希尔这样回信给葛瑞夫。

135

但是希尔并未完全轻视拉马努扬，他回信中的一些评论鼓舞拉马努扬继续去碰碰运气，因此拉马努扬直接将自己的东西寄给剑桥的数学家。其中两人因为无法看透拉马努扬奇怪语言背后的能力，直接拒绝了这个印度人的要求。但是有一封信来到了哈代的桌子上。

数学总是容易引发人们的奇思怪想，也许费马难逃其咎。为了应对宣称证明费马大定理而要求获得沃尔夫斯凯尔奖的众多奇怪来信，朗道的标准回信就证实了这一点。对于收到那些不请自来的、包含疯狂数字命理学理论的信件，数学家是屡见不鲜。哈代的朋友斯诺（C. P. Snow）回忆说，哈代也曾被那些信件骚扰，那些人宣称自己解决了金字塔神秘的咒语问题，以及培根隐藏在莎士比亚剧作中的密码。

拉马努扬经常与马德拉斯的一位数学教授加纳帕西·伊尔（Ganapathy Iyer）讨论数学问题，后来他从伊尔教授那里得到一本书——哈代的《无穷的等级》（*Orders of Infinity*）。当拉马努扬读到哈代的书时，他肯定意识到终于有人可以理解自己的思想，但他也承认自己害怕那些无穷和会让哈代“告诉我该去的地方是疯人院”。当拉马努扬看到哈代在书中说“到目前为止，还没有发现明确的公式，可以描述小于给定数的



素数个数”时，他觉得很兴奋，因为他已经发现了一个公式，他相信可以很精确地估计素数个数，他非常希望知道哈代对这个公式的看法。

当哈代在早晨发现这封盖着印度邮戳的信件时，第一印象并不是很好。其中的手稿包含着潦草的、奇怪的有关素数的定理，同时也包括了已知的著名定理，但是却被当作是原始发现记载。在手稿的封面上，拉马努扬宣称自己已经“发现了一个可以精确描述素数个数的公式”。哈代知道这是一个不寻常的宣言，但是手稿中并没有提供任何公式，更糟的是，没有任何证明！对哈代而言，证明就是一切。他曾在三一学院对罗素说，“如果我能从逻辑上证明你会在五分钟之内死去，我肯定对此感到十分伤心，但是我却会因为证明了这一点而感到稍许安慰。”

136

据斯诺所说，哈代很快浏览了拉马努扬的手稿，“这不光枯燥无聊，而且令人生气，看上去像骗子的作为。”但是到了晚间，这些疯狂的定理开始发挥它们的魔力。哈代在晚饭后叫来利特伍德一起讨论，到了午夜时分，他们终于破解了这份手稿。在破解了拉马努扬的非正统语言之后，哈代和利特伍德认识到，这些结果并非出自一个疯人之手，而是一份天才的作品，虽然未经训练，但却是非常杰出的成果。

他们两人知道，拉马努扬看似疯狂的无穷和实际上是对如何定义黎曼 ζ 函数中丢失部分的再发现。破解拉马努扬公式的关键在于将数 2 写成 $1/(2^{-1})$（(2^{-1} 是1/2 的另外一种表示方式）。利用这一点，哈代和利特伍德重写了原先的无穷和公式如下

$$1+2+3+\cdots+n+\cdots=1+\frac{1}{2^{-1}}+\frac{1}{3^{-1}}+\cdots+\frac{1}{n^{-1}}+\cdots=\frac{1}{12}$$

只要仔细观察，就可以发现这正是黎曼将数 -1 代人 ζ 函数后得到的结果。由于缺少正规的训练，拉马努扬只能孤身一人进行这些探索，并且重新发现了黎曼做出的关于 ζ 函数的结果。

拉马努扬的这封信来的正是时候。因为朗道的著作，哈代和利特伍德正着迷于黎曼 ζ 函数与素数之间的关系。在早晨哈代还认为拉马努扬宣称的结果——一个描述给定数之内的素数个数的不可思议的公式——



只是拉马努扬个人的奇思妙想，但是晚间的努力为了解这位印度人的手稿打开了另一扇门。

拉马努扬断言，自己的公式对于100 000 000以内的素数个数，“在大部分情况下是准确的，个别情况下的误差也就是1或者2。”这一论断深深地震惊了哈代和利特伍德，但是拉马努扬并没有给出任何公式。实际上，对于这两位坚持严格证明的数学家而言，这封信本身就已经是一件麻烦事，其中充斥着公式和命题，但是没有任何的验证或者是解释，说明它们从何而来。

哈代写了一封肯定的回信给拉马努扬，要求给出那些有关素数的公式的证明和详细内容。利特伍德在其中夹了一张字条，要求拉马努扬给出那个素数个数的公式以及“尽可能多的证明”。两位数学家期待着拉马努扬的回信，同时在许多个夜晚努力破解第一封信中的内容。罗素在给一位朋友的信中写道，“在学院大厅里我发现哈代和利特伍德处于一种莫名的兴奋之中，因为他们相信自己发现了第二位牛顿，一位拿着20英镑年薪的、印度马德拉斯的办事员。”

拉马努扬的第二封信适时抵达了英国，其中包括了几个关于素数个数的公式，但是仍然缺少证明。“这真是让人十分气愤！”利特伍德这样写道，他猜测拉马努扬应该是害怕哈代剽窃他的发现。当哈代和利特伍德开始研究第二封信时，他们发现拉马努扬又提出了一个黎曼已做出的结果。黎曼对高斯的素数公式的改进非常精确，并且黎曼发现利用ζ函数中的零点可以消除自己公式中的误差。在无人帮助的情况之下，拉马努扬部分地再现了黎曼在50年前提出的公式，他的公式包含了黎曼对高斯素数公式的改进，但是没有包括黎曼用ζ函数零点所作的那些修正。

拉马努扬的意思是否意味着这些零点产生的误差会以某种神秘的方式互相抵消？傅里叶已经为这些误差做出了音乐上的描述，每个零点代表着一个音叉，当这些音叉同时振动时，它们产生的就是素数的音乐。有时如果它们能互相抵消，声波也能产生寂静。飞机就是通过在机舱内



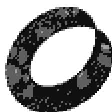
产生声波来抵消引擎的噪音。拉马努扬是不是在宣称这些零点产生的波最终发出的是寂静？

在复活节假日里，利特伍德带了一份拉马努扬信件的副本去康沃尔郡，和爱人及家人度假。“亲爱的哈代”，他这样写道（他们两人从来不称呼对方的名字），“关于素数的那些东西是错的。”利特伍德证明了这些波产生的误差没有办法互相抵消，因此拉马努扬的公式并不是像他宣称的那么精确。无论多大的数，总是存在着一定的误差。

受到拉马努扬信件的启发，利特伍德进行的分析导致了他对黎曼工作的新的了解。黎曼假设对于数学家而言变得更加重要，因为它意味着，在 N 以内高斯公式与真实素数个数之间的差，与 N 的大小相比较将会很小——实际上并不超过 N 的平方根。但是如果存在某些零点落在黎曼临界线之外，误差将会变大。在拉马努扬的信中，提到了也许可以做得比黎曼更好——对于更多的素数，误差比 N 的平方根要小很多。但是利特伍德在康沃尔郡的工作粉碎了拉马努扬的希望。利特伍德证明了在无穷多种情况下，零点产生的误差不会小于 N 的平方根，因此黎曼假设是最好的结果。虽然拉马努扬犯了错误，但是却留给哈代深刻印象。后来他写道，“在某些方面我并不确定，他的失败是否比成就更加奇妙。”

138

“关于他的错误如何产生，我有一个模糊的想法。”利特伍德在给哈代的信中猜测，拉马努扬自己的 ζ 函数图像世界中并没有那些位于海平面的点。如果这一点属实，那么拉马努扬的公式就是准确的。尽管如此，利特伍德仍然很高兴，他将拉马努扬比成黎曼时代的另一位数学大师，宣称“我相信他至少可以成为另一个雅各比”。哈代在写给拉马努扬的信中说道：“你声称的那些结果，有些已经得到了证明，并且都已经在数学史上留下了伟大的丰碑。”很显然，虽然拉马努扬具有惊人的才能，但是他急切地需要有人能将他带入现代数学的范畴，熟悉那些最前沿的知识。利特伍德在给哈代的信中谈到了自己的预感：“如果拉马努扬将来被素数中所蕴涵的恶之面俘虏，那是不足为奇的。”哈代对此评论道：“作为一个贫苦和孤独的印度人，他面临的形势极其困难，他



要用自己的头脑与西方世界多年来积累的智慧思想竞争。”

因此哈代和利特伍德决定不惜任何代价将拉马努扬带到剑桥。一位三一学院的同事内维尔（E. H. Neville）被派去劝说拉马努扬加入研究小组。起初拉马努扬并不愿意离开印度，因为作为一名虔诚的婆罗门教徒，他相信穿越海洋的旅行将使他失去贵族身份。他的一位朋友纳拉雅纳·伊尔（Narayana Iyer）知道拉马努扬渴望去剑桥，但是又不敢突破宗教传统，就帮他想了一个办法。伊尔知道，综合拉马努扬对数学的投入和对女神 Namagiri 的虔诚，也许可以产生意想不到的效果，能够说服拉马努扬去剑桥。于是他带着拉马努扬去 Namagiri 的神庙，去请求女神的旨意。在石头地板上睡了三天之后，拉马努扬突然惊醒，叫醒自己的朋友，“我看见一束亮光，女神命令我去剑桥。”看到自己计划的实现，伊尔开心地笑了。

拉马努扬同时也担心自己的家人不同意自己去剑桥，不过女神 Namagiri 再次发挥了作用。拉马努扬的母亲梦见自己的儿子坐在一间大房子中，周围都是欧洲人，女神 Namagiri 命令她不要挡着儿子的路。现在拉马努扬唯一的担心就是，在剑桥是否要应付那些烦人的考试。在内维尔打消了他的顾虑之后，拉马努扬终于可以离开马德拉斯，去往剑桥的学院和图书馆，这正是她母亲梦到的那一幕。

剑桥的文化冲突

1914 年，拉马努扬来到了剑桥，开始了数学史上最著名的合作。哈代经常兴奋地谈起与拉马努扬的合作，他们互相探索对方的数学思想，高兴地发现彼此都拥有相似的精神——那就是对数的热爱。后来哈代将与拉马努扬共度的这段时光认为是生命中最快乐的时光，并认为他们的关系“如同生命中一场浪漫的恋爱”那样令人难忘。

哈代和拉马努扬的合作类似古代的辩论组：其中有一个正方，一个反方。正方是永远的乐天派，有着许多疯狂的建议；反方则是悲观主义



者，怀疑一切，搜寻那些藏在袖子中的扑克。对拉马努扬而言，在他们交流自己的数学想法时，他需要的就是像哈代这样严格的人，来检查他粗糙的思想。

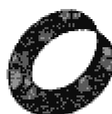
但是找到共同点并不容易，因为其中涉及文化的冲突。哈代和利特伍德坚持严格的、西方风格的证明；而拉马努扬的定理则是来自女神Namagiri的启发。哈代和利特伍德经常搞不懂这位新伙伴的想法是从何而来。哈代说，"当他几乎每天都交给我六七个新定理的时候，再对他是如何发现那些已知定理感到奇怪，好像就显得荒唐了。"

拉马努扬要面对的远远不止数学文化上的冲突。在一个充满学者和教授的世界中，他像外星人一样孤独。他难以找到素食，因此只好写信回家，让家人寄来罗望子和椰子油。如果不是因为他熟悉的数学世界，转变根本不可能发生。曾在印度得到拉马努扬信任的内维尔这样描述拉马努扬在剑桥最初的日子，"他对于生活在一个奇怪的文化社会中感到些许的苦恼：陌生的蔬菜不好吃、26年无拘束的脚正受着鞋的折磨。但是他是一个乐观的人，总是陶醉在自己的数学世界中。"每天都可以看见他穿着拖鞋走过校园，完全不见英国鞋的踪影。有一次有人看到在哈代的屋里，他自由地想象着自己的公式和方程，而哈代则盯着拉马努扬的笔记本，被那些迷人的定理所吸引。拉马努扬用自己孤立的印度数学，换来了剑桥独孤的文化氛围，但是却为他赢得了一位伙伴，一位能够探索自己数学世界的伙伴。

140

哈代发现对拉马努扬的教育难以产生平衡的效果。他担心如果坚持要求拉马努扬去证明那些结果的话，"也许会毁了他的自信或者破坏他产生灵感的魔力"。哈代交给利特伍德一个任务——让拉马努扬熟悉现代的严格数学。但是利特伍德发现这个任务根本就不可能完成，不管利特伍德讲什么内容，拉马努扬总是会产生无穷无尽的新想法，使得利特伍德不得不中断自己的讲课。

拉马努扬给出的素数个数的公式，曾帮助他实现去英国的愿望，最终他在相关领域作出了杰出的成果。在看到了哈代和利特伍德关于素数



是多么难缠的悲观评论之后，拉马努扬决定放弃对素数的正面攻击。现在我们只能推测，如果拉马努扬没有感受到西方学术界对素数的恐惧，也许能取得更加惊人的成就。后来，他与哈代一起探索了数论的其他方面。他们两人最初的结果有关哥德巴赫猜想——每一个偶数都可以写成两个素数的和，虽然这个结果并不直接，但它来自拉马努扬的直觉。拉马努扬的直觉坚信肯定存在某个公式可以精确地表示那些重要的数列，比如说素数。在当初那封含有素数公式的信中，拉马努扬也表示了自己知道如何生成另外一个尚未被驯服的数列——分划数。

有多少种不同的方法将五块石头分开？最多只能分为五堆，每堆一块石头；最少为一堆五块石头；以及介于两者之间的所有可能：

141

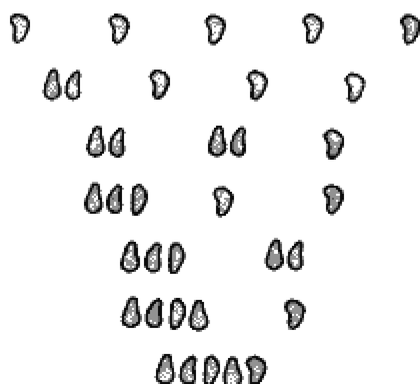


图 27　分开五块石头的 7 种方法

这些被称为 5 的分划。如图中所示，一共有 7 种可能的方法对 5 进行划分。

下面是数 1 到 15 的分划个数：

数	1	2	3	4	5	6	7	8	9	10
	11	12	13	14	15					
分划个数	1	2	3	5	7	11	15	22	30	42

56　77　101　135　176

这正是我们在第二章中碰到的数列，它们在物理世界中出现得与斐波纳契数列一样频繁。比如说，在某些简单的量子系统中能级密度就涉及理解这些分划数如何增长。

这些数看上去并不像素数那样随机分布，但是与哈代同时期的人费尽心思，最终还是放弃了寻找生成这个数列的公式的想法。退而求其次，数学家认为至少应该有一个公式能够大概估计这个分划数，但是又不会有太大的偏差。高斯的素数公式给出小于 N 的素数个数的一个较好的估计，也是基于同样的想法。但是拉马努扬对这些数列一点也不害怕，他一心要找出一个能准确地告诉你，有 5 种方法分划 4 块石头，或者有 3 972 999 029 388 种方法分划 200 块石头的公式。

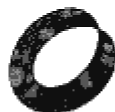
虽然拉马努扬在素数领域失败了，但是他成功地解决了分划数的问题。一方面是因为哈代处理复杂证明的能力，另一方面则是拉马努扬对肯定存在这样一个公式的固执坚持，促成两人完成这个伟大的发现。利特伍德根本就不能理解“为什么拉马努扬这么肯定这个公式的存在”。当我们看到这个包含 2 的平方根、π、微分算子、三角函数、虚数等内容的公式时，一定会奇怪这样的公式怎么可以想象出来：

142

$$p(n)=\frac{1}{\pi\sqrt{2}}\sum_{1\leqslant k\leqslant n}\sqrt{k}\Big(\sum_{h\bmod k}\omega_{h,k}\,e^{-2\pi i\frac{hn}{k}}\Big)\frac{d}{dn}\left[\frac{\cosh\left(\frac{\pi\sqrt{n-\frac{1}{24}}}{k}\sqrt{\frac{2}{3}}\right)-1}{\sqrt{n-\frac{1}{24}}}\right]+O(n^{-1/4})$$

后来利特伍德如此评论，“我们将这个定理视为是两个人非同寻常的愉快合作的结果，在其中两人都贡献了自己最好的、最有个性的以及最幸运的工作，这与馈赠完全不同。”

但是这里还有一点小问题。哈代和拉马努扬的这个复杂公式并没有给出正确的结果，离这个公式产生的结果最近的整数才是我们需要的。比如说，往这个公式中代入 200，离它输出的结果最近的整数是



3 972 999 029 388。但是这个公式已经足够好，因为它可以推导出正确的答案；但是令人苦恼的是它并没有彻底俘获分划数。（不久之后，有人发现对这个公式进行一些修正将得到准确的结果。）

尽管拉马努扬无法在素数上发挥这个技巧，但是与哈代关于分划数的合作研究可以给素数理论中的另一大未解难题——哥德巴赫猜想带来深刻影响。许多数学家放弃了尝试求解这个难题，因为解决这个问题的方法或手段都没有出现。数年之前，朗道也曾断言这个问题无法解决。

哈代和拉马努扬关于分划数的工作开创了一门新的技术，现在被称为哈代-利特伍德圆方法。这个名称来自于拉马努扬和哈代为了在虚数的附近进行积分计算而作出的一些小圆。但是为什么是利特伍德名字而不是拉马努扬的名字，这是因为正是他和哈代一起利用这个方法为证明哥德巴赫猜想做出了重要的贡献。虽然他们不能证明每个偶数都可以表示成两个素数之和，但是在 1923 年他们两人一起证明了一个结果，这个结果对于数学家而言也是同样美妙：取定一个足够大的数，那么比它大的所有奇数可以写成三个素数的和。但是他们这个结果还需要一个前提条件，就是黎曼假设成立。在黎曼假设没有成为黎曼定理之前，这个结果同样不能成立。

拉马努扬也帮助发展了这套方法，可惜他却没有能活到目睹该方法在数学中发挥重要作用的那一天。到了 1917 年，拉马努扬的情绪变得更加低落。由于英国当时正受到第一次世界大战的威胁，罗素因为持有反战观点而被取消教职；同时三一学院也不打算接纳拉马努扬的和平主义态度，拒绝为拉马努扬提供教职。尽管拉马努扬努力让自己的脚适应了英国鞋，并且生活在学者和教授的环境中，但是他仍然有着南印度人的灵魂。

拉马努扬习惯了在印度的那种自由生活，那里温暖的气候可以让人获得更多的户外时光。与之相比，剑桥就像一个监狱。他不得不躲在厚厚的大学校园围墙的里面，以躲避北海上吹来的凛冽寒风。除了学术圈子里的正规交流之外，他的社交圈子几乎为零。同时他也开始发现哈代



对数学的严格性要求，阻止了自己的思想自由地在数学世界中徜徉。

伴随着精神状态的衰落，拉马努扬的身体状况也逐渐走下坡路。三一学院无法理解拉马努扬严格的宗教饮食习惯。学院的厨房为像哈代和利特伍德那样的成员提供相同的服务，但是这对拉马努扬而言并非美食。同时，他无法适应一个人的生活，当他在印度的时候，他的妻子总是为他准备好了一切。想起在印度的妻子和家庭，他感到非常的孤单。营养失调导致他患上了结核病，不得不住进了疗养院。

拉马努扬试图继续思考数学问题，却没有什么成果。他的梦中充满了混乱的数学图像，他相信自己胃部的疼痛与黎曼图景中的无穷多个峰值紧密相连，在这些峰值处，ζ 函数趋向于无穷。是否这就是他违背了婆罗门的训诫，穿越海洋的惩罚？是否他误解了 Namagiri 女神的意思？自从他到了剑桥之后，他的妻子就没来过一封信，这样的压力已非一个常人所能承受。

在稍有恢复之后，拉马努扬的情绪仍然低落。他曾试图跳下地铁自杀，幸亏一位警卫及时发现，制止了地铁的运行，列车及时停在平躺在地铁上的拉马努扬前方。在 1917 年的那个时代，自杀也属于犯罪行为。但是哈代的介入使拉马努扬逃过了指控，但是他必须去德比郡马特洛克镇的一家疗养院进行 12 个月的全天候医疗监护。

144

拉马努扬被困在了疗养院，哪儿都不能去，甚至也不能与哈代进行每日的数学讨论。“我已经在这里待了一个月”，拉马努扬写信给哈代，“每天都不能思考数学问题，他们曾允诺会给我时间进行数学研究，但这一天总是不来，而我只能呆在这个讨厌的、寒冷的屋子里。”

最终哈代设法把拉马努扬转移到伦敦附近普特里的一家疗养院中。尽管哈代承认拉马努扬是自己一生中最好的朋友，但是他们之间的感情更多的是表现在讨论数学时体现的激情之上。即使在哈代去看望病倒在床上的拉马努扬的时候，也没有说出太多安慰的言语，而是谈到了自己来时乘坐的出租车号。哈代认为 1729 是一个没有多大意思的数，虽然拉马努扬仍在病中，但思维并没有停止，“不对，哈代！不对，哈代！



这个数很有趣，它是能以两种方式表示为两个三次方之和的最小整数。"拉马努扬是正确的，因为 $1729 = 1^3 + 12^3 = 10^3 + 9^3$。

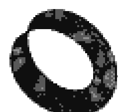
由于拉马努扬幸运地被选为英国最有名的学术团体——皇家学会——的成员，他最终获得了三一学院的教职。哈代在这些选举中的影响正是他所谓的爱的表现。但是拉马努扬并没有因此恢复健康，第一次世界大战结束时，哈代建议拉马努扬回印度修养一段时间。1920 年 4 月 26 日，拉马努扬在马德拉斯去世，年仅 33 岁。病因则可能是他在去英国之前就已经患上的一种大肠疾病阿米巴病。

虽然拉马努扬最终无法成功地征服素数，但他写给哈代的第一封信仍然有着延续不断的影响。数学家承认这个未解难题的答案随时随地都可能出现，一种新的想法可能会将之前隐藏的未知内容带到聚光灯下。但是拉马努扬的先例也说明，有时知识和期望也会妨碍数学的前进，那些建立在传统学习基础之上的学院课程并非总是创新的最好来源。总有这样的可能，某天有另外一个包裹来到某位数学家的桌子上，宣告着另外一位天才已经准备好完成拉马努扬的梦想——破解素数的密码。

145

拉马努扬留下的思想，足够数代数学家进行不断的研究。实际上，只在最近几十年内人们才充分认识到拉马努扬思想的真正价值。即使是在哈代去世的时候，拉马努扬公式的重要性仍然没有显现。哈代本人也忽略了拉马努扬的一个重要猜想，并在一篇文章中评论说"看上去我们好像漂到了数学的逆流处"。但是多年后，这个被称为拉马努扬 τ（Tau）猜想的重要性，可以从最终解决它的皮埃尔·狄利津（Pierre Deligne）被授予 1978 年的菲尔兹奖得到证明。一位拉马努扬的支持者，布鲁斯·本特（Bruce Berndt）将拉马努扬比作数学界中的巴赫，因为他们两人在死后多年都未被人们承认。

本特曾花大半生的时间研究拉马努扬未出版的数学笔记，他也是众多着迷于拉马努扬发现的大量公式和方程的数学家之一。在他研究这些笔记的时候，他发现了一张 100 000 000 以内的素数表，其中绝大部分素数都是正确的，少数错误的数也非常接近于正确值，并且比拉马努扬



第一次寄给哈代的那个公式生成的素数要准确得多。但是他求出这些素数的方法在笔记中却没有任何提示。

是不是拉马努扬已经得到了某个秘密的素数公式，像他的分划数公式一样有效？是不是能在他的笔记中发现另外的线索？1976年，整个数学界兴奋地发现了拉马努扬的一本丢失的笔记，其中是全新的数学内容。它的发现使我们更愿意猜测，可能在三一学院的旧文献或马德拉斯的箱子中会藏着更多的宝藏，它们也许可以解释拉马努扬为何能如此准确的计算素数的原因。

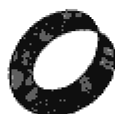
拉马努扬的死对哈代而言是一个巨大打击。因为哈代两个月前收到的信，还是"乐观的语气和数学"。失去了如此好的在数学领域中一起跋涉的旅伴，哈代觉得非常伤心，"自从我认识他之后，他的独特思想就是源源不断的建议来源，他的去世是我一生中受到的最大打击。"

当哈代变得年老，他也逐渐变得意气消沉。他一直以为自己还是年轻人，但是现在他不得不面对自己苍老的面孔，以至于在进入屋子之后都要收起所有的镜子。他还痛恨年老对自己数学能力的影响，《一个数学家的自白》正是他在数学生涯结束之时对此感觉的一份记录。要做数学，一位数学家"一定不能太老。因为数学是一门创造性学科而不是冥想的学科。没有任何人在他失去能力或者不再有创造愿望时还可以从数学这一学科中获得慰藉。而这种失去能力与创造愿望的情况可能会很快地在一个数学家身上发生"。

146

像拉马努扬一样，哈代也曾试图自杀，只不过是通过服药的方式而不是跳下地铁站台。但是他吐出了药丸，留下黑色的眼圈。斯诺后来回忆自己去探访病中哈代时的情景，"他自嘲说，他搞得一团糟，没有人比他搞得更糟了。"如他在《自白》中写到的那样，拉马努扬是对自己的安慰，"当我失望地却又不得不听那些浮夸而令人厌倦的谈话时，我就会对自己说：'哼，我做了件你们从未做过的事，那就是与利特伍德和拉马努扬在某种平等条件下的合作。'"

147



第七章

数学的迁徙：从哥廷根到普林斯顿

数学科学是如此庞大和分支众多，有必要进行针对性的培养，因为所有的人类活动都与什么地点和什么人有关。

——希尔伯特，

在1913年欢迎朗道担任哥廷根教授聚会上的讲话

朗道的父亲，莱奥坡·朗道（Leopold Landau）在柏林自己居住的街道上发现一位数学神童。莱奥坡·朗道对他很有兴趣，于是邀请这位神童来家里喝茶。虽然卡尔·路德维格·西格尔（Carl Ludwig Siegel）是一个害羞的孩子，但是他还是答应去见这位伟大的哥廷根数学家的父亲。在他的图书馆里，莱奥坡·朗道拿出儿子写的一套两卷本素数书籍给西格尔，并解释说，也许现在这本书对你而言太难，但以后你就能看懂了。这两卷朗道的书被西格尔视若珍宝，并在他后来的数学研究中产生了持续不断的影响。

西格尔18岁的时候正赶上第一次世界大战。当时参军报国的宣传冲击着他年轻的、内向的心灵，他对此十分害怕，并且深深厌恶一切有关战争的东西。除了朗道父亲培养的数学兴趣之外，他最初的愿望是在柏林学习天文学，因为在他看来，天文学不可能与战争有任何关系。只是天文学的课程迟迟未开，为了打发时间，他只好选修一些数学课程。不久他就深深地迷上了数学，并渴望探索数字宇宙的奥秘。很快，他就能够阅读朗道父亲给他的那本有关素数的书了。



到了1917年，战争不可避免地影响到了西格尔的生活。在他拒绝为军队服务之后，他被送往一家精神病院进行治疗。朗道的父亲设法将他救了出来，后来西格尔承认，“如果不是朗道先生的话，我很可能已经死了。”1919年，这位还未从伤痛中恢复的年轻人来到哥廷根，见到了自己的数学偶像朗道，从此他的数学才能开始得到充分的发挥。

西格尔发现自己必须学会容忍朗道那种独特的性格。在西格尔已经成名后的一天，他去柏林访问朗道。在晚宴上，朗道花费了整个用餐时间不停地解释一个极其复杂和有技巧的证明，并且详尽到每一个细节。西格尔耐心听着，当朗道完成自己的证明时，已是深夜。西格尔错过了最后一班公共汽车，只好步行回家。在回家的路上，西格尔思考着朗道的证明，这个证明同样是关于海平面上的点，其函数图像与黎曼图像类似。当西格尔回到家的时候，他想出了一个更加漂亮的证明，可以取代那个令他错过汽车的冗长证明。第二天，西格尔斗胆给朗道寄去了一张明信片，感谢他昨日的招待，并附上自己的证明概要，仅仅就在一张明信片上。

当西格尔回到哥廷根的时候，德国已经不堪战争消耗的重负，他只好和系里一位教授合住。另外一位教授帮他买了一辆自行车，以便他能方便地上班。最初哥廷根的数学等级制度令西格尔小心翼翼，特别是伟大的希尔伯特。因此他总是自己单独做研究，希望能做出某些突破，让这些大人物注意到自己。他参加了希尔伯特的讨论班，吸收着这位伟大人物的思想，他知道只要自己能解决23个问题之一就可以得到通往成功的通行证。

一开始，西格尔很害怕在大人物面前出现，如同在希尔伯特讨论班上那样。不过他最终鼓起勇气，接受了几位高级教师的邀请，去莱茵河参加他们的游泳活动。在游泳的时候，希尔伯特表现得一点也不可怕，于是西格尔有机会和他分享自己关于黎曼猜想的想法。希尔伯特热情地与他进行了交流，并且支持这位害羞的数学家于1922年在法兰克福大学获得了一个职位。



在西格尔的一生中，他成功地为一系列希尔伯特问题做出了贡献。但是正是他在希尔伯特第八问题——黎曼假设——上取得的非传统成就，奠定了他在数学史上的地位。

对黎曼的再思考

当西格尔开始投身希尔伯特第八问题的时候，他知道有些数学家已经逐渐了解到黎曼在这方面的贡献。西格尔的导师朗道也许是最坦白的批评家。尽管他熟知黎曼那份出版于1859年的十页论文，也知道这也许是“最杰出和具有最丰富内容的论文”，但是他还是有所保留，“黎曼的公式并非素数理论中最出色的结果，他只是为我们提供了一件工具，对它的改进可以让我们证明许多其他问题。”

149

同时在剑桥，哈代和利特伍德也表示了类似的意见。不过到了20世纪20年代，由于无法解决黎曼假设，哈代变得很沮丧。利特伍德也开始怀疑，是否他们无法证明这个结论，就意味着它其实是不正确的：

> 我相信这是不对的。没有任何证据可以支持它，我们不应该相信没有证据的事情。我必须记录我的感觉，没有任何可想象的原因表明它是正确的……虽然如此，如果真能确信它是不对的，那生活将会舒服许多。

如果要给出证据说明，所有的零点都落在黎曼假设所预测的那条线上，实际上黎曼也不能做到这一点。在他那份十页的论文中，连一个关于海平面上的点的计算都没有。哈代相信黎曼关于函数世界中零点的结论只不过是他直观的推测而已。

在这篇论文中黎曼没有进行任何零点位置的计算，其真实原因也许是因为黎曼认为一个真正思考、真正有思想的数学家不应该在这些枯燥的计算上浪费时间。毕竟，这是黎曼开创的革命的本质。希尔伯特也同样献身于推动这一数学的新潮流。正如他在一篇文章中写道的，“我已



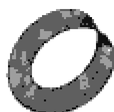
经尽力避免库默尔（厄斯特·库默，Ernst Kummer，狄利克雷在柏林大学的继任者）那些巨大的计算设备，因此这里也可同样实现黎曼的原则，即证明的动力应该仅仅来自于思想而不应该来自于计算。”希尔伯特在哥廷根的同事克莱因总爱说黎曼的工作是基于“最基本的思想”并且“经常依赖于自己的直觉”。

然而，哈代对直觉并不相信。他和利特伍德曾试图发展一种方法，来计算最初的那些零点的准确位置。如果黎曼假设是错的，那么利用这个公式，应该有一定的机会能找到一个零点，它落在黎曼临界线之外。黎曼曾发现在穿过1/2的那条临界线两侧，向东的世界与向西的世界存在着对称性，哈代和利特伍德的方法就利用了这个对称性。利用这个方法以及欧拉发明的一种估计无穷和的有效方法，到了20年代末，剑桥的数学家成功地确定了138个零点的位置。正如黎曼预测的那样，它们都落在穿过1/2的那条直线上。很显然，哈代和利特伍德的公式完全没有起到作用，而对于比这138个点更北方的点，精确计算它们的位置也变得难以实现。

150

看上去这些计算已经不能再推广。哈代通过理论分析证明了，无穷多个零点都必须落在临界线上。因此大家都承认，要想找到落在这条临界线之外的零点，必须去函数世界中更北方的地方寻找。正如利特伍德已经证明的那样，素数比起数学动物园中的其他生物，更擅长于在大范围的数字宇宙中隐藏自己真实的色彩。因此，数学家只好放弃去确定每个零点的准确坐标的想法，开始关注于其他对函数世界更理论的分析，来揭示黎曼思想中的那些神秘之处。

但是一次意想不到的发现改变了一切。当西格尔在法兰克福用自己的思想攻克黎曼假设时，他收到一封来自数学史学家埃力克·贝赛尔-哈根（Erich Bessel-Hagen）的信，当时贝赛尔-哈根正在研究黎曼那些未出版的手稿。尽管黎曼尽职的管家烧毁了他的大部分手稿，但是有一部分被黎曼的妻子伊莉斯抢救下来，她将其中大部分关于科学的手稿送给了黎曼的同时代人戴德金。数年之后，她后悔将这些有可能包含黎曼



个人隐私的手稿交给别人，于是她要求戴德金退回手稿。即使某份手稿的绝大部分内容都是数学，但只要包含了暗示某次购买商品的名称，或某个家庭成员的名字，也被伊莉斯要求退回。

剩下的科学手稿最终被戴德金存放到了哥廷根的图书馆。贝赛尔-哈根试图搞清这些大量手稿中包含的结果，但是结果很不理想。如同大部分数学家的私人手稿一样，混乱的、未成熟的思想与公式堆积在一起。贝赛尔-哈根希望西格尔能将这堆混乱的手稿破解。

西格尔给这位哥廷根图书管理员回信，询问是否可以浏览黎曼的遗作。经过努力，这位管理员将文献寄到了西格尔所在的法兰克福当地图书馆。西格尔对此任务很是盼望：因为他这段时间的研究一直没有什么进展，利用这件事可以让他从暂时的挫折中转换一下思想。包裹到了之后，西格尔和另一位访问学者一起急忙赶往图书馆。打开包裹，里面是乱糟糟的一堆纸片，其中充满了大量复杂的数值计算结果。这些文献击破了以往的传言，在70多年里，黎曼被传说成是一位依靠直觉和概念的数学家，无法为他的思想提供强有力的证据。面对这一大堆的计算草稿，西格尔讽刺地说："这就是黎曼伟大的一般思想！"

151

先前一些数学家为了寻找黎曼假设的线索，已经浏览过这些手稿，但是谁也无法从这堆手稿的方程中理清头绪。最令人奇怪的是，大量的算术计算似乎是黎曼在业余时间完成的。那么这些手稿涉及了什么问题？这就需要像西格尔这样的数学家来揭示黎曼所做的一切。

当西格尔开始阅读这些手稿时，他发现黎曼的研究同样符合他导师的格言。正如高斯一直强调的那样，当完成了一座建筑物之后，建筑师总是将那些原始的脚手架拆除。现在在西格尔手中的那些散落手稿则充斥着许多基础计算，由于黎曼生活很艰苦，在后期还要接济他的姐姐，因此他只能用差一些的纸，并且几乎所有的空白都被写满。希尔伯特所认为的思想家其实是一位计算大师，正是基于这些计算，黎曼构建了那些概念性的世界观，找出已知证据之间的规律。黎曼的一部分计算并无创新之处，比如说将2的平方根算到小数点后38位，但是西格尔却被



一些从未见过的计算激起了兴趣。当他进一步地研究这些手稿时，这些混乱的、毫无规则的计算好像有了一些意思。西格尔开始意识到黎曼是在计算零点。

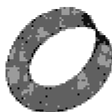
西格尔发现，黎曼使用的一个特殊公式能准确计算出 ζ 函数图像中点的高度。公式的第一部分是基于哈代和利特伍德已经发现的一个技巧，只是黎曼在 60 多年前就已经掌握了；公式的第二部分则是全新的：黎曼发明了一种新方法，用来计算无穷多项的和，这个方法比当时所用的方法要好很多。对比曾用来计算 138 个位于 ζ 函数图像中位于海平面的点的欧拉方法，在更远的北方，黎曼的方法更加有效。

即使在黎曼去世 65 年后，最著名的数学家仍然无法与之竞争。哈代和朗道曾错误地认为，黎曼的论文仅仅是个人非凡洞察力的体现。实际上，黎曼的论文是基于可靠的计算和理论思想，只是黎曼没有表明它们而已。在西格尔发现黎曼的秘密公式之后数年内，哈代在剑桥的一位学生利用它证实了前 1041 个零点都落在黎曼的临界线上。此后，该公式也随着计算机时代的到来发挥了它的实力。

152

说来奇怪，数学家居然花费如此长的时间才认识到，黎曼的手稿中很可能包含着一些珍宝。在黎曼的那份十页论文中，或是他写给其他数学家的信中，曾经有一些暗示，表明他不是凭空猜测。在论文中，他提到了一个新公式，但是他接着说自己“还需要将其进一步简化后再发表”。哥廷根的数学家研究这份论文超过 70 年，仍然对此一无所知，其实只需要再向前走几步就可以发现这个奇妙的计算零点位置的公式。克莱因、希尔伯特和朗道总爱对黎曼进行评论，但是没有一个人能花点时间看看这些未出版的手稿。

实话说，只要稍微看看黎曼的手稿就可以了解到这项工作的重要性。正如西格尔写的那样，“黎曼关于 ζ 函数的手稿都不适宜出版，偶尔可以发现一个公式散落在一页的不同地方，更常见的是一个公式只写了一半。”整个手稿看上去就像一部交响曲的最初草稿。要是没有西格尔的数学能力，从黎曼大量的笔记中提取出这个公式，也就无法得到最



后的结果。该结果也就因此得名：黎曼-西格尔公式。

由于西格尔的坚持，黎曼的另一面得到了展现。毫无疑问，黎曼是抽象思维和一般理论的大师，但是他同样知道不能忽视计算和数值试验的能力。他从来没有忘记自己所受的18世纪的传统数学教育。

存在哥廷根图书馆的黎曼手稿只是从管家手中抢救下来的一部分。伊莉斯·黎曼于1875年5月1日写信给戴德金，希望要回那些涉及个人隐私的部分手稿，其中包括了“一本记录了黎曼1860年春在巴黎所写内容的黑色笔记”。在这之前，黎曼匆忙发表了那份著名的关于素数的十页论文，目的是赶上柏林科学院的选举。后来在巴黎，没有着急出版的压力，黎曼有机会整理一下自己的思想。巴黎的天气十分恶劣，冰雹和暴雪使得黎曼没有时间在城里游玩，只好呆在家里将自己的思想记录下来。因此可以合理地猜测，在那本“黑色笔记”中，除了有个人的巴黎游记之外，肯定会有对那些 ζ 函数图像中位于海平面的点的想法。虽然有一些传说，但是这本笔记再也没有出现。

153

黎曼的女婿在1892年7月22日写信给亨里克·韦伯（Heinrich Weber）说：“起初母亲并不能接受公开黎曼手稿的这个想法。对她而言，这些东西是神圣的，不应该让学生随意观看，因为其中也许有一些注记涉及个人隐私的问题。”费马的侄子很希望能出版叔叔的那些注记，但是黎曼家族却不愿意公开那些黎曼不愿意发表的内容。由此看来，这本黑色笔记应该还是在家族成员的手中。

关于这本笔记的所在的猜测有很多种。有证据表明贝赛尔-哈根从黎曼家族成员的手中获得了一些未出版的材料，但是我们不清楚他是从拍卖会上还是通过私人关系得到这些材料。其中一部分材料最终流落到柏林大学的档案室，但是贝赛尔-哈根似乎要将另外一部分变成自己的收藏品。在第二次世界大战结束后的混乱中，贝赛尔-哈根于1946年冬天死于饥饿，他的收藏也不知所踪。

另一个版本的故事说，这本黑色笔记辗转流传到了朗道的手中。据说，在不确定的战时年代里，朗道将这本笔记给了自己的女婿数学家勋

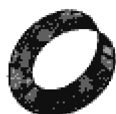


博格（I. J. Schoenberg），勋博格于1930年逃往美国，从此就没有这本笔记的消息。鉴于目前有着百万美元的悬赏，寻找黎曼失踪的黑色笔记在某种意义上也成为一场寻宝之旅。

如果没有黎曼的那些手稿以及西格尔的决心，要找出如此神秘的公式又将花去我们多长的时间？这个公式是如此的复杂，也许直到今天也无法发现。如果那本黑色笔记没有失踪，我们又将发现多少珍宝？黎曼曾说自己可以证明绝大部分的零点都落在临界线上，直到今天，没有一个人能够重现这个证明。在德国图书馆的档案库中又藏着多少秘密？黑色笔记是不是流落在美国？这本笔记逃过了管家的大火，但是却没能逃过第二次世界大战的战火？

到了1933年，在德国的数学家发现越来越不能集中精力研究数学。万字旗飘扬在哥廷根图书馆的上方。由于学校中有不少犹太人和左翼人士，当时街头的游行都将矛头指向数学系，称之为“马克思主义的堡垒”。到了30年代中期，由于希特勒对校园的清洗运动，大部分教师失去了工作，不得不到海外寻找庇护。朗道虽然是犹太人，但是由于他是在第一次世界大战前被任命的教授，才得以保留工作，因为在1933年4月通过的“公职法案”中的非雅利安条款对于终身教授或参加过战争的人并不适用。

但是形势逐渐恶化。到了1933年冬天，朗道的课程受到纳粹学生的监视，学生中包括了后来的著名数学家奥斯瓦德·梯奇缪勒（Osward Teichmüller）。一位哥廷根的犹太裔教授说梯奇缪勒是“一个非常年轻、有科学天分的人，但是也是很糊涂和带点疯狂的人”。有一次，当朗道抵达教室时，他被这位年轻的纳粹成员拦住了。梯奇缪勒告诉朗道，他讲授微积分学的犹太方式完全不符合雅利安人的思维方式。朗道承受不了这样的压力，于是辞职来到柏林。对朗道而言，无法任教不啻为人生的一个重大打击。后来哈代回忆邀请朗道去剑桥教课时的情形，“看到当他再次站到黑板前时显露出来的高兴，与他不得不离开时显露出的悲伤，这样的对比让人十分感伤。”由于不忍远离自己的家乡，朗道又回



到了德国，并在1938年去世。

那一年，没有任何犹太关系的西格尔离开法兰克福来到哥廷根，挽救数学系岌岌可危的声誉。但是到了1940年，西格尔也不得不流亡美洲以表达自己对战争的抗拒。经历了童年时期恐怖的第一次世界大战，西格尔曾发誓，如果自己的祖国再次牵涉到战争中，他将永远不再回来，因此在第二次世界大战时期西格尔呆在普林斯顿的高等研究院。那些建立了哥廷根伟大声望的数学家，现在只有希尔伯特仍留在德国。他喜欢哥廷根在数学界的统治地位，并且作为一位老人，他不能理解周围所发生的灾难。西格尔曾向他解释为什么周围的同事纷纷离开的原因，“我感觉他认为我们是在和他开玩笑”，西格尔回忆说。

在数个星期内，希特勒毁灭了由高斯、黎曼、狄利克雷和希尔伯特建立起来的伟大的哥廷根传统。一位时事评论员认为这是“从文艺复兴以来人类文化史上最严重的灾难”。自从受到30年代纳粹德国的破坏之后，哥廷根（也许应该加上德国数学）就再也没有得到复兴。在目睹了哥廷根的中世纪街道被摧毁的一幕后，希尔伯特死于1943年的情人节。他的死标志着哥廷根作为数学圣地年代的结束。

155

纵观整个欧洲，数学都陷入了危机之中。当自己的国家在准备面对不可避免的战争之时，为了自己的爱好继续追求抽象概念，也变得越来越不可能。再一次，欧洲的科学开始为国家的军事需求服务。而许多的数学家则像西格尔那样，从欧洲来到美洲。他们发现在大西洋的彼岸，繁荣的国家和政策的支持正是进行纯粹研究的最佳环境。这种学术迁徙的受益者是美国，自此数学的中心再也没有回到欧洲。

当战争结束的时候，有些数学家结束了流亡生涯，回到了自己的家乡。西格尔也回到了德国。由于呆在普林斯顿，他对欧洲数学的发展一无所知，认为在他离开的时间中应该没有什么进展。可是事实并非如此，当大部分数学家离开欧洲或者停止研究工作时，仍然出现了一条大新闻。在西格尔碰到玻尔，也就是哈代在哥本哈根攻克黎曼假设时的合作伙伴时，他问这位老朋友：“那么，在我呆在普林斯顿的时候，有什

么情况出现吗?”玻尔的回答很简单:“塞尔伯格!”

塞尔伯格:孤独的斯堪的纳维亚人

1940年,挪威的奥斯陆大学邀请西格尔去当地举办一次讲座,而西格尔正想借这个机会去往普林斯顿。德国政府同意了这次访问,并没有意识到西格尔正是以此为跳板逃离欧洲,登上从奥斯陆去往美洲的轮船。当轮船离开港口的时候,西格尔看到一队德国商船正抵达挪威,后来他听说这正是德国侵略挪威的先头部队。西格尔成功地逃离了欧洲,但是在奥斯陆大学数学系里有一位年轻的数学家正埋头于数学之中,完全无视外面的混乱现实,他的名字叫做阿特尔·塞尔伯格(Atle Selberg)。

156

在战争降临挪威之前,塞尔伯格就习惯于将自己关在家中进行研究。隐居的生活常常会迫使数学家进入一个全新的领域。塞尔伯格决定从事的数学领域,在他周围的人都不熟悉。无人相助的事实并不能阻止他,相反,他对于单枪匹马的工作已经很习惯了。当战争逼近,挪威与外界断绝了一切联系,因此也无法得到国外的科学杂志。对此,塞尔伯格认为是一个激励,“这就像在监狱中一样,你与世隔绝,从而可以全神贯注于你的工作,不会被他人的工作影响。从这一点来看,我认为这种状态对于做自己的工作还是相当不错的。”

这种自足的态度贯穿了塞尔伯格整个的数学人生。这种态度形成于他的青年时代,当时他非常愿意一个人呆在父亲的书房中,钻研书架上的许多数学书。正是在那时,塞尔伯格读到了挪威数学会学报上一篇关于拉马努扬的文章。塞尔伯格回忆说那是“奇怪但又很优美的公式……给我留下了极深的印象”。拉马努扬的工作成为塞尔伯格的主要动力,

157

“这就像是一个启示——一个全新的世界出现在我的面前,给了我很大的想象空间。”作为礼物,他的父亲送了一本《拉马努扬论文集》给他,直到今天塞尔伯格还将它带在身边。通过自学以及父亲大量的数学



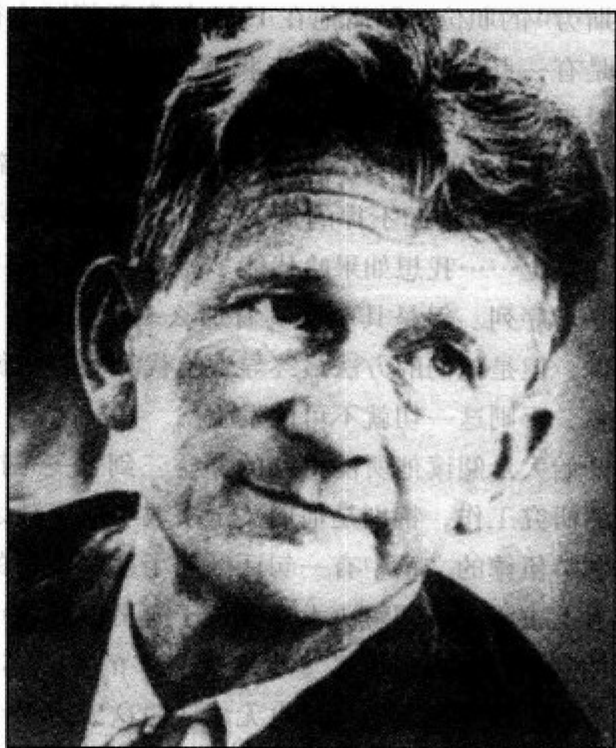


图 28　阿特尔·塞尔伯格，普林斯顿高等研究院教授

藏书，在 1935 年进入奥斯陆大学之时，他已经能够做出原创的结果了。

塞尔伯格对拉马努扬与哈代一起做出的关于分划数序列的公式特别感兴趣。尽管拉马努扬的这个公式被认为是惊人的成就，但是其中仍然有些微小的不足：利用这个公式得到的结果并不是一个整数，离结果最接近的那个整数才是分划数。显然应该存在这样一个公式，它的结果恰好就是分划数。1937 年的秋天对塞尔伯格而言是快乐的，因为他做出了比拉马努扬更进一步的结果，找到了分划数的准确公式。不久他读到了对自己这篇文章的审稿意见，令他大失所望的是，他在终点线前输给了别人。一位叫做汉斯·拉德马彻（Hans Rademacher）的数学家已经在前一年发表了相同的结果。因为持有和平主义，德国纳粹政府停止了拉



德马彻在布雷斯劳①的职位，随后他在1934年离开德国去往美国。"当时这对我来说是有一点打击，不过后来我就渐渐习惯了。"这件事也说明当时挪威相对于主流数学发展的孤立状态。

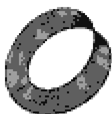
对塞尔伯格而言，哈代和拉马努扬会错过准确公式简直是不可思议。"我确信哈代对此有推卸不掉的责任……哈代并不是完全相信拉马努扬的洞察力和直觉……我想如果哈代能多相信拉马努扬一点，他们肯定能得到拉德马彻序列。但是其中确实有那么一点怀疑。"也许事实就像塞尔伯格所说，但是他们的方法最终导致哈代和利特伍德在哥德巴赫猜想上做出贡献，否则这一切就不可能发生。

塞尔伯格开始大量阅读他所能得到的剑桥三剑客——拉马努扬、哈代和利特伍德的研究工作，特别是他们关于素数与ζ函数之间联系的工作。在哈代与利特伍德的文章中有一句话激起了塞尔伯格的兴趣，他们说目前的方法看上去没有希望解决大部分位于海平面的零点是否落在黎曼的临界线上的问题。哈代证明了至少有无穷多的零点落在临界线上，这是一大步的跨越。即使如此，哈代也无法证明这无穷多个零点是所有零点的一个分数。抛开哈代和利特伍德做出的一些改进，这些可以证明的零点个数相比于那些无法证明的零点个数，只是沧海一粟。因此他们断言，用自己的方法无法对结果进行根本上的改进。

158

但是塞尔伯格并不像哈代和利特伍德那样悲观，他认为从他们的方法中仍然可以发掘出新的东西。"我看着哈代和利特伍德的原始论文，到最后他们解释为什么这个方法无法给出进一步结果的原因。我一边读一边思考，然后意识到他们的观点是完全没有道理的。"塞尔伯格预感到自己可以走得比哈代和利特伍德更远。虽然他还无法证明所有的零点都落在临界线上，但是他可以用自己的方法证明存在一个确定的比率，并且随着向北方考虑更多的零点，这个比率不会缩小为零。塞尔伯格并

① Breslau，德国城市，现名弗罗茨瓦夫。1945年，弗罗茨瓦夫因《波茨坦条约》的签署而归属波兰。



不确定这个比率究竟是多少，但是这的确是首次结结实实地从这块硬骨头上咬下了一块，并且留下了清晰的牙印。想象一下，你可以知道塞尔伯格证明了大概有百分之五到百分之十的零点落在临界线上，当你向北方考虑更多的零点时，至少有这么一个比率的零点满足黎曼假设。

虽然这并不是黎曼假设的证明，但塞尔伯格的进展仍然是心理上的一个突破。不过这个结果并不为外界所知，因为塞尔伯格不确定这是否又是别人已经证明的结果。在战争结束后，塞尔伯格被邀请参加1946年夏天于哥本哈根举行的斯堪的纳维亚数学家大会。由于在发现分划数的准确公式这件事上已经受到过打击，他决定最好确定一下这个关于零点的结论究竟是新的还是旧的。但是奥斯陆大学还没有收到那些因战争而延误的学术杂志，“我听说特隆赫姆[①]理工学院的图书馆有这些杂志，于是我专程跑了一趟特隆赫姆，在那里的图书馆呆了一个礼拜。”

现在塞尔伯格不用担心了，因为他发现自己在关于黎曼 ζ 函数零点的问题上已经远远走在别人的前面。他在哥本哈根的报告证实了玻尔对美国来访者的断言，欧洲战时的数学新闻就是“塞尔伯格！”塞尔伯格演讲的内容是自己关于黎曼假设的研究结果。虽然他已经为证明黎曼假设做出了一个不小的贡献，但是塞尔伯格也认为实在是没有太多的事实能支持黎曼假设的正确性。“我想大家那么愿意相信黎曼假设的正确性，本质上还是因为这个命题的优美和分布的简单性。沿着临界线你可以看到对称性，它还与素数的分布有关，在这个宇宙中至少有一些东西是正确的吧。”

159

有些人误解了塞尔伯格的评论，认为他在散播怀疑黎曼假设正确性的言论。但是塞尔伯格不像利特伍德那样悲观，认为缺少证据的支持就意味着黎曼假设不正确。“我一直强烈地认为黎曼假设是正确的，我永远也不会怀疑它。但是在当时情况下，我认为既没有一些真正的数值结果也没有理论结果来严格支持它的正确性。所知的结果也只能说明它在

---

① Trondheim，挪威中部港口城市。



很大程度上是正确的。”这就是说，也许大多数的零点落在临界线上，这也正是黎曼在接近一个世纪之前宣称的结果。

塞尔伯格在战时做出的突破，代表着欧洲在数学界统治地位的最后辉煌。随着塞尔伯格的成功，他被普林斯顿高等研究院的一位教授看中，这位教授是赫尔曼·外尔（Hermann Weyl），外尔在1933年离开形势恶化的哥廷根。这位留在欧洲的孤独数学家，忍受了“二战”期间的穷苦生活，无法抵挡来自大洋彼岸的橄榄枝的诱惑，于是塞尔伯格接受了邀请，出发访问高等研究院。怀着即将得到全新灵感的兴奋之情，塞尔伯格抵达了繁忙的纽约港，驱车前往曼哈顿南部的安静小镇——普林斯顿。

像塞尔伯格这样的从大洋彼岸流入的数学家，为美国数学的发展带来了极大的好处。曾经是数学穷乡僻壤的美国，逐渐占据了数学的主流地位。直到今天，它还是世界数学的中心，吸引着来自全球的数学家。虽然哥廷根作为数学界圣地的名誉被希特勒和第二次世界大战摧毁，但是它将在普林斯顿的高等研究院像凤凰一样重生。

高等研究院（The Institute of Advanced Study）成立于1932年，由路易斯·般博格（Louis Bamberger）和姐姐卡罗琳·般博格·富尔德（Caroline Bamberger Fuld）捐赠500万美元兴建而成。它的目标是吸引世界上最优秀的学者，提供给他们一个天堂般的工作环境和可观的薪水——实际上，它有一个绰号叫做“高薪水研究院（The Institute of Advanced Salaries）”。高等研究院试图复制牛津和剑桥的学术气氛，让来自不同领域的专家从交流中得到提高。

相比较于那些稍显陈腐的传统学术环境，普林斯顿的空气是年轻且新鲜的，充满着生机与新思想。在牛津或剑桥的高桌上谈论自己的工作被认为失言，但普林斯顿并没有如此挑剔。研究院的成员只要愿意，可以在任何时候公开谈论自己的工作。爱因斯坦认为普林斯顿是一个未被熏过的烟斗，“普林斯顿是一个令人惊讶的地方，在这里你可以看到立柱顶端的小小神像。但是抛开这些社会传统，我可以为自己创造一个研



究环境，保证不被打扰。在这个小小的大学城，可以远离人类战争的喧嚣。”

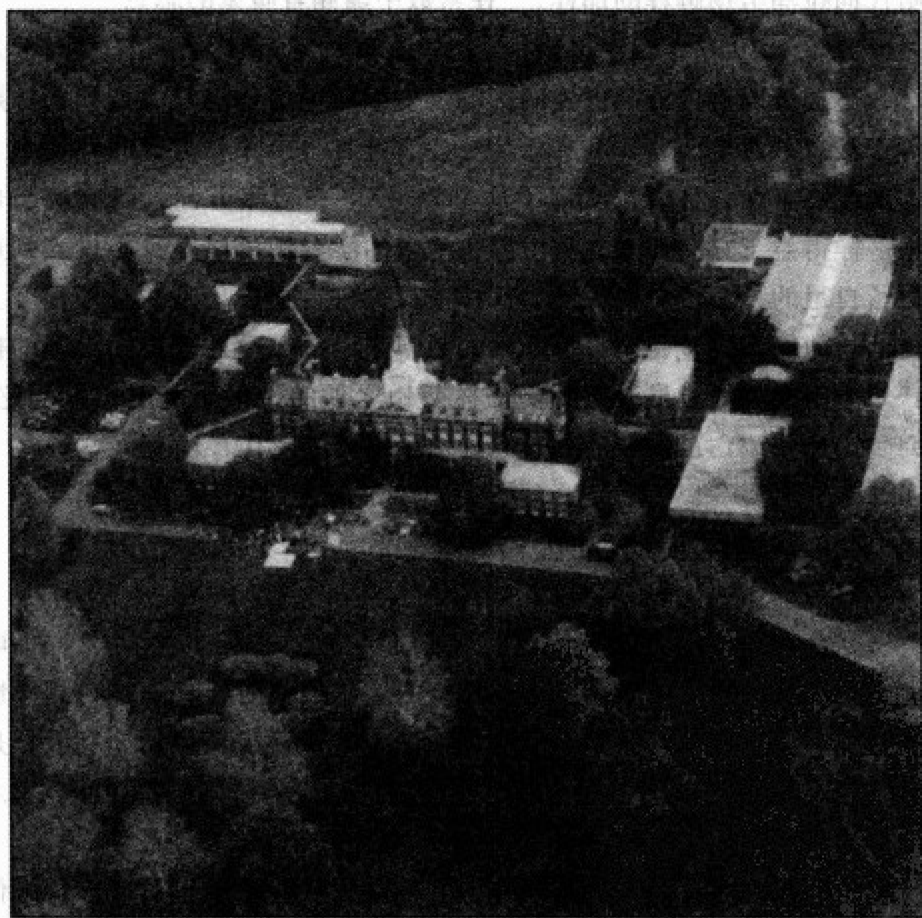


图 29　普林斯顿高等研究院

研究院成立的宗旨是要涵盖所有的学科，但是它却成立于普林斯顿大学的数学系大楼中。数学系则在后来搬往普林斯顿的最高建筑法恩楼(Fine Hall)。因此研究院也可能受到所在地的影响，数学与物理学科特别突出。在教师休息室的壁炉上刻着几行字，是爱因斯坦经常引用的，



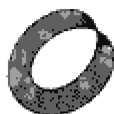
“Raffinieri ist der Herr Gott, aber boshaft ist Er nicht（上帝是难以捉摸的，但是他并无恶意）”。但是数学家对这样的论断还是存在着不少怀疑，正如哈代向拉马努扬解释的那样，“在素数中蕴涵着魔鬼的恶意”。

研究院于1940年搬迁，新地点坐落在普林斯顿的郊区，周围都是树林，更加可以避免外部世界的影响。爱因斯坦描述自己流亡到普林斯顿等于被“放逐到天堂，我曾希望一生都能在一个不受打扰的环境中工作，现在终于在普林斯顿实现了这个梦想”。在很多方面，研究院与哥廷根一样得益于它的孤立，从世界各地来的学者们可以全身心投入到这个自给自足的社会中。有人认为普林斯顿这种自给自足是在某种程度上的自信。他们不仅接受来自哥廷根的数学家，也接受这个德国小镇的格言：对于研究院的成员，不需要普林斯顿之外的生活。由于与世隔绝，研究院为那些流亡自欧洲的数学家提供了最佳的工作环境。

厄多斯：布达佩斯的巫师

研究院有一位来自欧洲的流亡数学家与塞尔伯格的生活发生了联系。当拉马努扬的故事激励了挪威年轻的塞尔伯格时，它的魔力同样影响了另外一位年轻人。保罗·厄多斯（Paul Erdös），一位匈牙利人，是20世纪后半期最有魅力的数学家。但是拉马努扬并非这两位数学家之间仅有的联系，他们之间曾有过一场数学论战。

塞尔伯格喜欢一个人进行研究，厄多斯则从合作中得益良多。人们经常会看到驼背的厄多斯，穿着随意的鞋子和衣服，出现在世界各地的研究所中，与自己新的合作者一起，埋头于笔记本中，沉浸在自己的热情之中，解决那些数论中的问题。厄多斯一生写过超过1500份论文，这是一项仅次于欧拉的惊人成就。厄多斯是一位数学苦行僧，他放弃了很多个人爱好，以免影响自己的研究；他将自己挣的工资发给学生，或者作为解出自己问题的奖赏。像哈代一样，上帝在厄多斯的世界观中占了一个非同寻常的地位。“至尊法西斯”是他给“圣书”管理员的外



号，“圣书”（The Great Book）则包含着所有已解或未解数学难题的最优美证明，厄多斯对一个证明最好的评价就是“圣书中就是这样的!”。他相信所有的婴儿——或者是他所谓的艾普希龙（ε），这个希腊字母常被数学家用来表示无穷小量——出生时都掌握了来自于“圣书”中关于黎曼假设的证明的知识。问题在于，6个月之后，他们都忘记了这一切。

厄多斯喜欢边听音乐边做数学，经常有人在音乐会上看见他在笔记本上潦草地书写，兴奋地记下那些新思想。尽管厄多斯是一位很好的合作者，并且讨厌孤独，但是他却讨厌身体上的接触。他享受着咖啡和咖啡因药片带来的精神上的愉悦，他曾这样说过，“数学家就是将咖啡转化为定理的机器。”

和许多伟大的数学家一样，厄多斯幸运地有一位好父亲，能够让他接触到新的思想，并激发出他对数论的热情。有一次，他的父亲向他介绍了欧几里得关于存在无穷多素数的证明时，利用欧几里得的思想证明了可以找到任意长度的区间，在其中不存在素数，这个结果深深地迷住了厄多斯。

如果你想找到由100个数组成的一串连续整数，其中不存在素数，只需要取所有101以内的数，然后将它们相乘，这个结果称为101的阶乘，记为101!。那么101！肯定可以被从1到101的任何数整除，因此如果N是1到101之内的数，那么$101!+N$肯定也可以被N整除，于是所有的数

$$101!+2,\ 101!+3,\ \cdots,\ 101!+101$$

都不是素数，这样我们就找到了100个连续的整数，它们全部不是素数。

厄多斯的兴趣被激发了，对于101!，你需要再数多少个数才能碰到下一个素数？欧几里得已经断言，肯定有一个素数在那里，但是是不是意味着在找到下一个素数时，我们需要数任意多个数？如果素数是由大自然扔硬币决定的话，我们确实无法知道从一个“正面”到下一个“正面”究竟有多远。当然，连续得到1000个“反面”是非常罕见的



——但是并非不可能。当厄多斯进一步研究时，他知道在这方面素数与扔硬币完全不同。它们看上去是一堆混乱的数，实际上它们的行为并非完全随机。

163

一位法国数学家约瑟夫·伯特兰（Joseph Bertrand）在1845年首次进行猜测，究竟需要走多远，才能保证碰到下一个素数。他相信如果你取任意一个数，比如1009，那么在你数到它的两倍时，你一定可以发现一个素数。实际上在1009和2018之间存在着很多素数，第一个是1013。那么对于任意的N，伯特兰的结果正确吗？他不能证明你总是可以在N和$2N$之间找到一个素数。但是这个预测是他在年仅23岁时作出的，因此这个结果被称为是伯特兰假定（Bertrand's Postulate）。

这个命题作为一个未解问题并不像黎曼假设那样长寿。不到7年的时间，俄国数学家帕努梯·切比雪夫（Pafnuty Chebyshev）给出了证明。其中的思想类似于切比雪夫当年进攻素数定理时的想法，当时他证明了高斯的猜想与真实素数个数之间的误差不可能超过百分之十一。切比雪夫的方法不如当年黎曼发展的那套方法精巧，但是非常有效。因此，不像扔硬币那样完全不能确定下一个“正面”何时出现，切比雪夫证明了总存在一个很小的范围可以预测素数。

厄多斯于1931年做出的第一个结果是关于伯特兰假定的新证明，当时他年仅18岁。但令他失望的是，有人告诉他应该参看一下拉马努扬的工作，结果他发现自己的证明并不像期望的那样是全新的，拉马努扬最后的工作极大地简化了切比雪夫关于伯特兰假定的证明。虽然年轻的厄多斯很失望，但是发现拉马努扬工作获得的喜悦盖过了失望。

厄多斯决定好好想想，是不是能够做得比拉马努扬和切比雪夫更好。于是他开始研究素数之间的间距究竟有多大，这也是厄多斯一生中一直感兴趣的问题之一。厄多斯的名声还来自于他乐于设立奖金，用来奖励那些解决自己猜想的人。他给出奖金1万美元用来征求一个证明，证明自己关于两个连续素数之间的间距究竟有多大的猜想。直到今天，尽管厄多斯已经无缘见到这个证明，这个问题仍然悬而未决，奖金也无



人认领。厄多斯曾开玩笑地说，当有一天这个问题被解决的时候，自己的奖金可能已经违反了最低工资法。有一次，厄多斯鲁莽地开出100亿阶乘美元的奖金，征求他关于高斯素数定理的一个推广猜想的证明（100亿阶乘是将1至100亿之间的所有数相乘后的结果）。要知道，100阶乘这个数已经远远超过了宇宙中所有的原子数。不过让厄多斯宽心的是，在20世纪60年代没有一个数学家能得到这份奖金。

当厄多斯在20世纪30年代末期到达高等研究院的时候，他很快就扬名立万。马克·卡克（Mark Kac）是来自波兰的避难者，虽然卡克感兴趣的是概率论，但是厄多斯对他的一次演讲发生了兴趣。卡克打算讨论一个函数，它可以描述当数越来越大时，有多少不同的素数可以整除某个数。比如说，15 = 3 × 5 可以被两个不同素数整除，而 16 = 2 × 2 × 2 × 2 只能被一个素数整除。因此对每个数，我们都可以记录究竟有多少不同的素数整除它。

厄多斯回想起哈代和拉马努扬曾研究过这些数如何变化，但是只有像卡克这样的一位统计学者才能看清楚这些数的完全随机的行为。对于越来越大的数，将每个数对应的素数个数记录下来并作出图像，卡克看出整个图像非常类似于统计学中的钟形曲线，这正是随机性的特征。虽然卡克辨认出了这个关于素数因子个数函数的行为，但是他却不能利用数论中的技巧来证明这个关于随机性的猜测。“我于1939年3月在普林斯顿首次报告了这个猜想。不仅是我的荣幸，也是数学界的荣幸，厄多斯就在听众之中。他立即开始思考，在报告完成之前，他已经完成了证明。”

这次成功激发了厄多斯对于数论和概率论的混合学科的终身热情。初看上去，这两门学科像粉笔和奶酪。哈代曾轻蔑地说，“概率根本就不是纯数学，而是哲学或者物理。”数论学家研究的对象是那些自从世界存在就永恒不变的对象，像哈代所说，不论我们喜欢或者不喜欢，317总是一个素数。另一方面，概率论则是最狡猾的学科，你永远也不知道下一步将会发生什么。



有序零点蕴涵随机素数

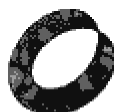
虽然高斯曾用抛硬币的思想来猜测素数个数，但直到20世纪数学家才开始考虑将完全不同的领域——概率论和数论——结合起来。在20世纪的最初几十年，物理学家发现几率是亚原子世界不可或缺的组成部分。一个电子的行为也许像一个极小的弹子球，但是你永远也不能精确测定它的位置。尽管许多物理学家对此很反感，但利用量子骰却能告诉你在何处可以发现这个电子。也许正是量子物理和关于世界的概率模型的出现，使得人们开始认为，几率是不是在某些决定性的学科——像素数理论——中也并非一无是处。当爱因斯坦拒绝接受上帝掷骰子的思想时，厄多斯在走廊的另一端已经证明了掷骰子存在于数论的核心之中。

165

实际上，也正是在这一时期，数学家开始理解黎曼假设。这个关于ζ函数图像中零点的整体性质的定理，解释了为什么素数看上去是那么的无序和随机。理解有序零点和随机素数之间相互作用的最好方法就是对随机性的模型——抛硬币——做更深入的研究。

如果你抛100万次硬币，会得到大概一半的正面和一半的反面，但是你永远也别想得到一个精确的数值。用一个完全随机、没有偏差的公平硬币，你会看到在50万次正面中会出现大概1000次的误差。如果这样的实验是基于完全随机的过程，概率论为测量这个误差的大小提供一种方法。如果抛N次硬币，那么将会在$N/2$个正面中或多或少出现一定的偏差（或称“误差”）。对于公平硬币，这个误差基本上和N的平方根同一数量级。比如说，掷100万次公平硬币，得到正面的次数基本上会是在499000至501000之间（1000是100万的平方根）。如果这个硬币存在偏差，那么产生的误差将会大于N的平方根。

高斯正是基于抛硬币的思想来估计素数的个数，只不过此时第N次抛出正面的可能性是$1/\log(N)$而不是1/2。由于在正常情况下，抛硬币的结果也不可能正好是1/2的正面和1/2的反面，因此自然界在抛素



数硬币时也不可能正好就是高斯预测的那个结果。但是误差是多少呢？是像抛硬币那样有一个控制范围，还是存在着比较严重的偏差，使得在某一段数中根本就找不到一个素数？

166

这个答案存在于黎曼假设之中，与零点的位置息息相关。这些位于海平面的点控制着高斯对于素数个数猜测的误差，每个东-西坐标为 1/2 的零点都会产生 $N^{1/2}$（这是 N 的平方根的另一种表示法）的误差。因此，如果黎曼关于零点位置的猜想是正确的，那么高斯对于素数个数的估计值和真实素数个数之间的误差最多和 N 的平方根同一数量级。这正是概率论中关于公平硬币完全随机行为的误差估计。

如果黎曼假设是错误的，则意味着一些零点落在黎曼临界线之外，那么这些零点产生的误差要比 N 的平方根大许多。这就像抛硬币时，得到的正面要多于背面，而不是公平硬币得到的一半对一半。如果黎曼假设不正确，则意味着素数硬币是不公平的，如果有零点落在临界线的东部越远，则素数硬币产生的偏差将越大。

公平硬币会产生完全随机的行为，而有偏差的硬币则会形成一种模式。因此黎曼假设抓住了为什么素数看上去如此随机的原因，黎曼杰出的洞察力将这种随机性转化为图像中零点与素数之间的联系。为了证明素数确实是随机的，你必须证明在黎曼照虚镜的另一边，零点是整齐地排列在那条临界线上。

厄多斯很喜欢黎曼假设的这样一个概率论的解释。一方面，它能提醒数学家为什么需要进入黎曼照虚镜背后的世界；另一方面，厄多斯还希望能够促使这些数学家重新关注数论的基本对象：数。自从黎曼开启了数学世界的虫洞，一个全新的数学世界出现在许多数学家的面前，此后只有很少的数论学家还关注于数论本身，他们更多关注的是黎曼 ζ 函数图像中的几何性质，以及寻找那些位于海平面的点，而不是谈论素数本身。厄多斯极大地改变了这一切，他是为了素数而研究素数，不久之后他发现在这条路上自己并不孤独。



数学论战

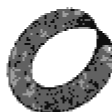
尽管塞尔伯格曾经着迷于黎曼的 ζ 函数，但是在普林斯顿时，他的兴趣从 ζ 函数转到了对素数的直接关注。随着数学向美洲的迁徙过程，他的兴趣也开始回到黎曼照虚镜的这一侧——更加实际的世界。

167

虽然瓦勒普桑和哈达马证明了素数定理，但是不存在一个简单方法证明高斯关于对数和素数之间联系的事实，令数学家非常失望。是不是只有利用黎曼 ζ 函数以及虚数图像这种特别复杂的工具，才能证明高斯对素数个数的估计？数学家无奈地认为也许只有这个工具才能证明，高斯的猜测正如黎曼假设所导出的那样，误差不会超过 N 的平方根。但是他们相信或许存在另外的简单方法来得到高斯给出的粗糙估计。切比雪夫曾经证明高斯的估计最多与真实素数个数相差百分之十一，数学家希望能在此基础之上得到进一步结果。但是 50 年过去了，无数寻找简单证明的尝试都以失败告终。数学家渐渐相信，黎曼引入的、瓦勒普桑和哈达马发展的这一套复杂工具在证明过程中是不可避免的。

哈代相信，高斯素数定理不存在一个初等的证明。并非哈代不希望这样，数学家的永恒追求是朴素的证明，哈代只是对此感到悲观，并且怀疑是否存在这样一个初等证明。如果他能多活几个月，他将会为看到厄多斯和塞尔伯格的贡献，找到了一个素数和对数之间联系的初等证明而感到欣慰。不过后来关于这个初等证明该归功于谁的争论，肯定会令哈代感到心寒。在很多地方都可以看到这个故事，其中两本是厄多斯的传记。由于厄多斯庞大的合作者和联系人网络，加上塞尔伯格的沉默，应该可知这个故事主要是以厄多斯的观点来讲述。因此，这里应当记述一下塞尔伯格在这个事件中的观点。

最先利用 ζ 函数这个复杂工具的数学家是狄利克雷，他用它证明了费马的一个猜测。狄利克雷证明了，如果取一个表面为 N 小时的时钟计算器，当你输入素数时，计算器的结果中会出现无穷多次 1。这也就是



说，存在无穷多个素数，它们除以 N 之后的余数是1。狄利克雷的证明依靠了 ζ 函数的复杂计算，这个结果也是黎曼伟大发现的催化剂。

168

1946年，在狄利克雷做出发现110年之后，塞尔伯格找到了狄利克雷定理的一个初等证明，其原理与欧几里得关于存在无穷多素数的证明很相似。塞尔伯格的证明避免了 ζ 函数，在当时许多人相信如果不使用黎曼的思想就无法在素数理论领域做出突破的情况下，这个结果是心理上的重大突破。这个证明虽然不太明显，但是它完全不需要任何复杂的19世纪数学，即使是古希腊人说不定也能看懂。

一位匈牙利数学家保罗·图让（Paul Turán）在访问普林斯顿高等研究院的时候与塞尔伯格成了好友。同时他也是厄多斯的朋友，实际上当苏联的巡逻队在1945年解放后的布达佩斯街头将他拦住时，他唯一能找到的代表身份的东西就是与厄多斯合作完成的一篇文章，这给巡逻队留下了深刻印象，以致后来图让在被送往古拉格监狱的途中被营救。他自己笑称这是“数论的一个伟大应用”。

图让渴望理解塞尔伯格关于狄利克雷定理证明背后的某些思想，但是他在春季结束时就要离开。于是塞尔伯格高兴地向他介绍了某些证明中的细节，甚至建议图让就此证明进行一次讲座，而他本人则要去办理去往加拿大的签证问题。但是在他和图让讨论的过程中，塞尔伯格谈到了更多的问题。

在讲座上，图让提到了塞尔伯格已经证明的一个特殊公式。这个公式与狄利克雷定理的证明并无多大联系，但是坐在下面的厄多斯却注意到这正是自己所要的公式，可以用来改进伯特兰假定，那个关于 N 与 $2N$ 之间存在素数的猜测。厄多斯希望做的问题是，是不是真的需要数到 $2N$ 才能得到下一个素数，也许你总可以在 N 和 $1.01N$ 之间找到素数。厄多斯也认识到这并不是永远成立，比如说，取 N 等于100，则在100与101之间连整数都没有，更何况是素数。但是厄多斯相信，如果 N 足够大，那么由伯特兰假定的核心思想，肯定存在一个素数位于 N 与 $1.01N$ 之间，并且1.01无任何特殊性，厄多斯认为只要是1与2之间的



任何数都可以。听到图让的讲座之后，厄多斯开始意识到塞尔伯格的公式为自己的证明提供了关键的一步。

169

"在我回来之后，厄多斯问我是否介意利用这个公式给出推广伯特兰假定的一个初等证明。"这只是塞尔伯格思考过的一个问题，但是他没有考虑过它的应用，"由于我并没有考虑这方面的问题，所以我说我没有意见。"当时塞尔伯格正被一大堆的实际问题困扰，他需要更新自己的签证，同时由于接受了下一年在锡拉丘兹[①]的职位，他必须在锡拉丘兹找到住宿的地方，另外还需要为一个工程学校准备夏季的课程。"无论如何，厄多斯在寻找证明方面都是相当的快。"

然而有些东西塞尔伯格并没有透露给图让。实际上，塞尔伯格会考虑伯特兰假定的推广问题的真正原因是他想利用它来完成素数定理的初等证明。有了厄多斯的结果，塞尔伯格现在已拥有证明所需的最后一块砖。

塞尔伯格告诉厄多斯如何利用厄多斯的结果完成素数定理的初等证明。于是厄多斯建议将这个工作在那些曾经参加过图让讲座的小范围听众中进行公布。但是，厄多斯实在控制不住自己的兴奋，发出了许多邀请，并保证这是一次非常有趣的讲座。另一方面，塞尔伯格并没有预料到如此众多的听众。

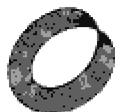
> 当我到达那里时，大概是下午四五点钟。屋里坐满了人。于是我走上讲台开始讲述证明的过程，然后我邀请厄多斯上来讲述他的结果，我好接下去完成这个证明。因为这个证明是利用了厄多斯得到的那个中间结果。

厄多斯建议两人合写一篇论文解释详细的证明。但是塞尔伯格这样解释，

> 我从来没有发表过合作论文，我希望各自单独发表论文。但是厄多

---

① Syracuse，美国纽约州中部一城市。



斯坚持要像哈代和利特伍德那样进行合作，对此我一直没有同意。我来到美国后，就像我在挪威时那样进行数学研究，一直是单独进行的，甚至不会和别人讨论……不，我并不是指那种意义上的合作，也许我会和别人谈论，但是我都是自己研究，这是与我的脾气相吻合的。

真相是这两位数学家拥有完全不一样的脾气。其中一位是完全自给自足的独行客，与印度数学家萨拉瓦达姆·周拉（Saravadam Chowla）的合作文章是其一生中唯一的一篇合作文章，并且也有违他的意愿。另外一位则极度看中合作研究。数学家经常会谈论起厄多斯数，这个数代表的是通过合作文章，自己与厄多斯之间最少需要多少步才能联系起来。如果某人的厄多斯数是3，则代表他与A合写过文章，A与B合写过文章，B与厄多斯合写过文章。由于周拉是厄多斯507位合作者之一，因此塞尔伯格一生中唯一的一篇合作文章赋予他厄多斯数2。有超过5000位数学家的厄多斯数都是2。

170

在这次拒绝之后，塞尔伯格承认“事情无法控制”。在1947年厄多斯已经建立了极为广泛的合作者网络，他经常利用明信片告知这些合作者自己的最新进展。当塞尔伯格到达锡拉丘兹的时候，一位朋友这样欢迎他的到来，“你听说了吗？厄多斯和某位斯堪迪纳维亚人已经给出了素数定理的初等证明。”当时，塞尔伯格已经发现了另外一种证明方法，可以绕过厄多斯提供的那个中间结果，于是他将这个结果单独署名发表在《数学年刊》（*Annals of Mathematics*）上。这份由普林斯顿大学出版的杂志被认为是世界上最权威的三本数学杂志之一，怀尔斯也正是在这本杂志上发表了自己对费马大定理的证明。

厄多斯被激怒了，他请求赫尔曼·外尔来主持公道。塞尔伯格叙述道，“我很高兴外尔在听取了两方的意见之后，最终站在了我的这边。”厄多斯发表了自己的证明，并在其中感谢塞尔伯格发挥的作用。但那是一个不幸的年代，抛开数学本身的超脱名利，数学家多少还是存在着一些自负，希望可以得到别人的奉承。对于创新的过程，将自己的名字永



远地与某个定理联系起来，这是最好的驱动力。塞尔伯格与厄多斯的故事说明了优先权在数学中的重要性，实际上在所有的学科中都是这样。这也是为什么怀尔斯可以在自己的阁楼里呆上7年，秘密地解决费马大定理，所有的一切都是为了防止别人来分享荣誉。

虽然数学家像接力比赛中的选手，传递着接力棒从上一代到下一代，但是他们仍然希望可以独享穿越终点线时得到的那份荣耀。数学研究就是在长期的合作需求和渴望永恒名誉之间的复杂平衡。

过了不久，人们渐渐清楚塞尔伯格关于素数定理的初等证明并非是人们期待的那个突破。有人认为，其中的某些思想也许可以提供证明黎曼假设的基本方法，毕竟这个想法可以证明高斯猜测和真实素数个数之间的误差不会超过 N 的平方根，并且人们已经知道这个命题等价于所有零点落在黎曼临界线上那个命题。

171

到了20世纪40年代末，塞尔伯格仍然保持着自己的纪录，证明有多少点落在黎曼的临界线上，这也是他获得1950年菲尔兹奖的原因之一。当时已经80岁的哈达马，被邀请参加在马塞诸塞州剑桥市[1]召开的国际数学家大会，见证塞尔伯格的成果。哈达马很渴望见到这位年轻人，因为他给出了初等方法，证明了自己和瓦勒普桑在50年前做出的结果。然而，哈达马和劳伦特·施瓦兹（Laurent Schwartz），另外一位菲尔兹奖的获得者，都因为有苏联背景而无法顺利得到签证——当时麦卡锡主义刚刚初露锋芒，最后是在杜鲁门总统的干涉之下，他们才恰好在大会举行的前一天被允许进入美国。

后来数学家利用一些新方法，推广了塞尔伯格关于有百分之多少零点落在黎曼临界线上的证明。如果你对前进的方向有了新想法，那么定理的证明就非常自然，最难的反而是该领域的最初一步。然而推广塞尔伯格的估计则完全不同，证明需要非常精细的分析，并非仅仅依靠一个

---

① Cambridge，又称坎布里奇市，位于美国马塞诸塞州，哈佛大学以及麻省理工学院所在地。



伟大思想的启发，而是需要坚持不懈的努力才能走到最后。前进的路上充满了陷阱，只要一步走错，那么原先大于零的数可能立刻就会成为负数，每一步都需要非常的小心，还要提防随时会出现的错误。

在20世纪70年代，诺曼·勒维森（Norman Levinson）改进了塞尔伯格的结果，并认为在某种程度下，自己可以掌握98.6%的零点的位置。勒维森将一份证明手稿交给在麻省理工学院的同事吉安-卡洛·罗塔（Gian-Carlo Rota），开玩笑说自己已经证明了100%的零点都落在临界线上——其中98.6%包含在手稿中，剩下的1.4%留给读者证明。罗塔以为他是认真的，便开始告诉大家勒维森已经证明了黎曼假设。当然，即使勒维森已经证明了100%的零点落在临界线上，那也不能够说明所有的零点都落在临界线上，因为我们这里涉及的是无穷多个零点。但是这条消息还是迅速地流传开了。

最终有人在手稿中发现了一个错误，零点的百分比因此下降到了34%。当然，这仍然是一段时间内的世界纪录，同时勒维森也因为在60多岁做出这个结果而名声大振。塞尔伯格说，"进行如此大量的数值计算说明他拥有超乎常人的勇气，因为事先并不知道结果会如何。"据说勒维森对如何推广自己的方法有个不错的想法，但是在将这个想法付诸实施之前他就因为脑瘤去世了。现在这个纪录属于俄克拉荷马大学的布瑞恩·孔瑞（Brian Conrey），他在1987年证明了有40%的零点必须落在临界线上。孔瑞同样对提高这个估计值有一些想法，但是他觉得仅仅为了提高几个百分比，而去做大量的计算是不值得的。"如果我能证明这个估计值大于50%，那么这个工作就是有价值的，因为这样我们就可以说大部分的零点落在临界线上了。"

172

对初等证明的归属权的争论，使厄多斯觉得很受伤，但是他仍然继续出产丰富的论文，向年龄老化和数学才能的枯竭挑战。当他失去普林斯顿的终生职位之后，他成了一名流浪数学家。由于没有住房和工作，他不得不去拜访那些遍布世界的朋友，来满足自己对合作的热爱，与他们呆数个星期之后又继续下一段旅程。厄多斯于1996年去世，正是素



数定理得到证明的百年纪念。即使是在83岁的高龄，厄多斯仍然发表合作论文，在去世之前他说，“至少还需要100万年，我们才能真正理解素数。”

现在，满头白发的塞尔伯格已经90多岁，但是他仍然关心黎曼假设的最新进展，不断地参加各种会议，提供思想给年轻的参会者。在他轻声的话语中你仍然可以听出他家乡挪威的语调，但是在此之下则是对别人工作深刻和尖锐的评论，因为他对愚笨的人没有什么耐心。在1996年，他在西雅图举办的证明素数定理百年纪念会议上所作的讲演，获得了全场600名数学家的热烈欢呼。

塞尔伯格相信抛开已有的这些进展，我们对如何证明黎曼假设还是无从下手：

> 有人也许会猜测我们是不是已经有了答案，或者说我们已经接近了答案。当然随着时间的流逝，如果我们已经得到了某个结果，那么就离目标更近一步，然而我并不这么认为。这与费马定理完全不同，现在还没有任何相关的突破。也许在半个世纪后的2059年也无法解决，当然我是无法目睹这一切了。这个问题还要保持未解状态多久，现在也不好说。我认为最终一定可以找到答案，并且这个答案是可以被证明的。也许这个证明相当复杂，以至于人脑无法理解它。

173

在战后于哥本哈根所作的报告中，塞尔伯格还曾对黎曼假设的正确性产生过怀疑。在那时，证明黎曼假设只是充满希望的想法，但是今天他的观念已经变化，50年之内出现的证据已经在塞尔伯格的脑中产生了决定性的影响。而正是在第二次世界大战时，特别是布莱切利庄园的密码破解者发明的机器——计算机——提供了这些新的证据。

174



第八章

思想的机器

我打算考虑这个问题，“机器能思考吗？”

——阿兰·图灵（Alan Turing）《计算机与智力》

阿兰·图灵的名字将永远与破译“二战”时期德国密码“Enigma”的事件联系在一起。在牛津和剑桥的中间，是悠闲的小镇布莱切利庄园（Bletchley Park）。在那里丘吉尔的密码破译员制造了一台机器，用来破译德国情报机构每日发出的消息。关于图灵成功地将数学逻辑和决定论联系在一起，成功地在德国潜艇的威胁之下挽救了许多生命的故事，一直是小说、戏剧和电影的素材。而关于创造“炸弹”（bombes）这台密码破译机的灵感来源，则可以追溯到图灵在剑桥的数学生涯，那个哈代和希尔伯特统治的年代。

在第二次世界大战席卷欧洲之前，图灵已经计划制造一台机器，用来解决希尔伯特23个问题中的两个。第一台机器是理论机器，仅仅存在于思想中，人们曾经希望数学大厦的基础可以被检验，但是这个希望被这台机器所摧毁。第二台机器则是实实在在存在的，由齿轮和润滑油构成。图灵希望利用这台机器挑战另一项数学难题。在图灵的梦想中，这台旋转的精密仪器或许可以推翻希尔伯特的第八问题，也是希尔伯特在23个问题中最关心的那一个：黎曼假设。

看到这么多年来自己的同事都不能证明黎曼假设，图灵认为也许是时候验证一下究竟黎曼假设是对是错。也许确实存在一个零点落在临界线之外，也正因此造成素数序列的某种规律。图灵知道机器将是搜寻零



点工作中最强有力的工具，也许因此就能推翻黎曼假设。多亏了图灵，现在数学家才拥有了一种全新的机器工具，帮助他们探索黎曼假设的奥秘。但并非只有图灵的现实机器对数学家探索素数产生过重要的影响，他那存在于思想中的机器，原先只是用来挑战希尔伯特第二问题的机器，在20世纪后期却产生了最意想不到的一个结果：生成素数的一个公式。

图灵对机器的热爱来源于一本书。1922年，在图灵10岁的时候，他得到的礼物是棒球，在一起的还有一本书——埃德温·坦尼·布鲁斯特（Edwin Tenney Brewster）所著的《每个儿童应该知道的自然奇观》，正是这本书激发了童年图灵的想象力。这本书出版于1912年，书中给出了自然现象的解释，但是并不仅仅是让小读者们被动地接受这些知识。布鲁斯特关于生命的描述特别地具有启发性，为将来图灵对人工智能的兴趣打下了基础：

175

> 当然，生命就是一台机器，是极其复杂的机器。虽然比任何手工制作的机器都要复杂千万倍，但仍然是一台机器。曾有人将生命比作一台蒸汽机，但那是在我们对生命工作原理了解之前的事，现在我们认为它是一台内燃机，就像是汽车、轮船和飞机的发动机一样。

在学校里，图灵热衷于发明和制作一些新东西：可以重新加墨的钢笔、甚至是打字机。直到他在1931年进入剑桥大学国王学院成为一名数学本科生，这些爱好仍然伴随着他。尽管图灵比较内向和孤独，和很多前辈一样，他在数学提供的绝对确定性之下找到了安全感。同时他对于发明创造的热情并没有减退，他一直关注着那些能揭示抽象问题结构的物理机器。

作为一名本科生，图灵研究的首个结果是试图理解抽象数学与奇异自然界交汇处的问题。他的出发点是抛硬币这个实际问题，而结果则是对任何随机实验所产生结果的复杂理论分析。像厄多斯和塞尔伯格那样，在完成自己的证明之后，图灵失望地发现这个结果已经在10多年



前由芬兰数学家林德博格（J. W. Linderberg）得到，并被称为中心极限定理。

后来数论学家发现中心极限定理为估计素数个数提供了全新的思想。黎曼假设曾断言，真实素数个数与高斯估计值之间的误差应该是与抛一枚公平硬币得到的误差相同；但是中心极限定理则揭示了素数的分布不可能用抛硬币模型来模拟。素数并不遵循中心极限定理对随机测量做出的修正。由于统计学从不同的角度来分析给定数据，因此从图灵和林德博格的中心极限定理的观点来看，虽然素数与抛硬币有很多共同点，但他们并不是一回事。

176

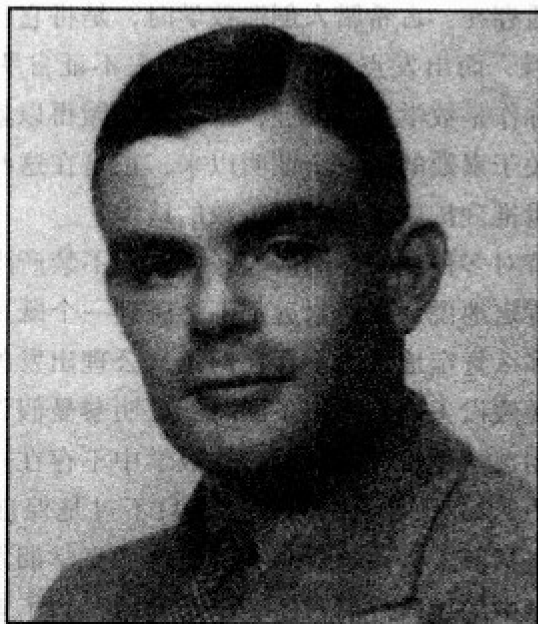
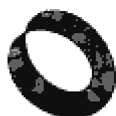


图 30　阿兰·图灵，1912～1954

图灵关于中心极限定理的证明虽然不是最早的，但已经足够证明他的才能，他也因此被选为国王学院的成员，那时他才 22 岁。不过在剑桥的数学圈子中，图灵仍然是孤独的。当哈代和利特伍德为数论中的经典问题奋战时，图灵宁愿在数学教条之外进行探索，与其阅读同时代人



的文章，他更愿意做出自己的结果。和塞尔伯格一样，他将自己排除在传统的学术圈子之外。

除了这种自加的孤独，图灵也注意到了正渐渐逼向数学的一场危机。剑桥的数学家纷纷讨论着一位年轻奥地利数学家的工作。数学曾经给予图灵安全感，但是现在某种不确定性却被放置到了数学的中心。

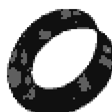
177

哥德尔和数学方法的局限性

在自己的第二个问题中，希尔伯特希望数学界能给出一个证明，证明数学中没有矛盾存在。古希腊人创造数学时，是将它作为由定理和证明构成的一门学科，而出发点则是那些看上去不证自明的关于数的真理。这些真理被称作是数学中的公理，是数学花园得以盛开的种子。自从欧几里得给出关于素数的第一个证明以来，正是在这些公理的基础之上数学家利用逻辑推理扩展了我们对于数的认识。

但是希尔伯特对多种几何学的研究，使我们不禁产生了这样一个问题，我们是否能肯定地说，我们永远都不会碰到一个既正确又错误的命题。我们究竟能多么肯定地认为不存在两条从公理出发的推理步骤，其中一条能证明黎曼假设正确，另一条同时能证明黎曼假设错误。希尔伯特肯定地认为利用数学逻辑可以证明，在数学中不存在这样的矛盾。在希尔伯特的观点中，23 个问题中的第二道只不过是保证数学大厦的整齐有序而已。在包括罗素——哈代和利特伍德的哲学朋友——在内的一些人发现某些数学中的矛盾之后，这个问题开始得到了重视。虽然罗素的不朽巨著《数学原理》找到了解决这些矛盾的一个方法，但却激发了更多人对希尔伯特第二问题的关注。

在 1930 年 9 月 7 日，希尔伯特被授予柯尼斯堡荣誉市民的称号，这是他热爱的故乡。这一年也是希尔伯特从哥廷根退休的一年。他在演讲的最后号召所有的数学家："Wir mussen wissen. Wir werden wissen."（"我们必须知道，我们也将会知道!"）在演讲之后，他被邀请去录音



棚将最后一段录下，以供广播播放。现在你可以在录音中“我们必须知道”后面听到希尔伯特的笑声。但是希尔伯特不知道的是，在他发出笑声的前一天，有一场会议在附近的柯尼斯堡大学召开，25岁的奥地利逻辑学家科特·哥德尔（Kurt Gödel）作了一场报告，这次报告彻底地摧毁了希尔伯特的世界观。

在童年时期，哥德尔被称为“Herr Warum”——问题先生——因为他总有着无穷的问题。儿时的风湿热给他的心脏带来了影响，并留下永久的抑郁症。到他晚年的时候，抑郁症变成了完全的偏执狂。他总是认为有人试图毒害他，于是他绝食直至死亡。但是在他25岁时，哥德尔摧毁了希尔伯特的梦想，并导致了数学世界中的一场风暴。

178

在自己的论文中，哥德尔将自己的好奇心转向希尔伯特那些涉及数学核心的问题。哥德尔证明了，数学家永远不可能证明拥有希尔伯特所渴求的坚实的基础，利用那些数学公理永远也不可能证明这些公理不会导致矛盾。那通过修改某些公理或者加上一些公理，能不能改变这个状况呢？答案也是否定的。哥德尔告诉我们，不管为数学选择什么样的公理，它们都不能被用来证明其中不存在着矛盾。

数学家称一组公理是相容的，如果它们不会导致矛盾。我们可以在选择公理的时候，保证它们不会产生矛盾；但是在使用这些公理的时候，会不会得到矛盾就无人知晓。也许从某组公理出发可以证明相容性，但这只是一部分的成功，因为对于这组公理的选择的相容性仍然是一个问题。这就像希尔伯特希望通过将几何转化为数来证明几何的相容性，但是这导致的问题就是算术的相容性。

179

哥德尔的成就让我们想起在斯蒂芬·霍金的《时间简史》开头，一位老妇人描述的宇宙观。这位夫人站在一场通俗天文讲座的最后一排，声称“你告诉我们的都是无稽之谈，世界是在一头巨大乌龟背上的平坦表面。”而当报告人反问她这只乌龟是站在什么上面的时候，她笑了起来，“你很聪明，年轻人，非常聪明。乌龟是一个一个叠在一起的。”

哥德尔为数学提供了一个证明，说明数学世界是建立在一系列乌龟

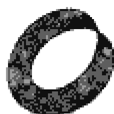




图 31　科特·哥德尔（1906~1978）与
阿尔伯特·爱因斯坦，1950 年

的背上。我们可以找到一个不会推导出矛盾的理论，但是我们不能证明在这个理论之内不存在矛盾。我们所能做的只是在另一个系统之内证明相容性，但是这个系统本身的相容性却无法被证明。数学居然被用来证明了自身的有限作用范围，法国数学家安德烈·魏伊（André Weil）精辟地描述了后哥德尔时代的现状，“上帝存在是因为数学的相容性，魔鬼存在则是因为我们无法证明这一点。”

希尔伯特在 1900 年宣称在数学中没有任何“不可知”的东西。30 年后，哥德尔证明了无知是数学不可分割的一部分。离开柯尼斯堡数月后，希尔伯特听说了哥德尔的结果，听到这个结果时，希尔伯特显然



"有些愤怒"。而希尔伯特在哥德尔演讲后一天作出的宣言"Wir mussen wissen. Wir werden wissen"最终也得到了它应有的位置。这句话作为一个理想主义者的梦想，也是数学最终兴起的动力，被刻在希尔伯特的墓碑上。

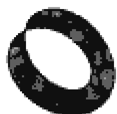
当时，物理学家正从海森伯的不确定性原理中认识到自己所认识的世界存在着许多限制。哥德尔的证明则意味着数学家也不得不与数学自身的不确定性生活在一起：也许有一天他们会发现整个数学体系只不过是海市蜃楼。当然对于大多数数学家而言，直到今天这一世界末日仍然没有到来，也许就说明这一切永远不会发生。我们有一整套有效模型来验证相容性，但是由于这套模型根本上是无穷多项，因此我们不知道究竟在哪一步与公理产生矛盾。正如我们看到的那样，在数的宇宙中，最简单的素数也隐藏着那么多的惊喜，并且这些惊喜无法通过简单的实验和观察来发现。

180

哥德尔并没有止步于此，他的论文包含着第二颗炸弹。如果数学公理是相容的，那么总存在着一些正确的命题不能由这些公理进行形式上的证明。这一点是与从古希腊以来整个数学界的观念相悖的，证明一向被认为是通往数学真理的道路，现在人们对证明能力的信心全部被哥德尔粉碎。有些人希望加上一些新的公理来修补数学大厦，但是哥德尔同样证明了这一切都是白费工夫，无论在数学大厦的地基上加上多少新的公理，总还是存在某些正确的命题无法被证明。

这被称为哥德尔不完全性定理（Gödel's Incompleteness Theorem）——任何相容的公理系统本质上都是不完备的，也就是说存在一些正确的命题无法由这些公理推出。同时，协助哥德尔实施这项数学恐怖主义行动的正是素数。哥德尔给每一个数学命题赋予素数作为其独立代码，称为哥德尔数。通过分析这些数，哥德尔就可以证明无论选择什么样的公理，总存在某些正确的命题无法被证明。

哥德尔的结果对全球的数学家而言都是一记重拳。由于存在着许多关于数，特别是素数的命题，它们看上去是正确的，但是我们却找不到



恰当的方法去证明。哥德巴赫猜想就是其中之一：每一个偶数都是两个素数的和；孪生素数猜想：存在无穷多对素数，就像17和19那样，它们的差为2。是不是像这样的命题，都会成为那些在现有公理体系上无法证明的命题吗？

不可否认，这确实是令人失望的形势。也许黎曼假设在我们现有的算术公理系统中就是无法证明。许多数学家安慰自己那些真正重要的命题都应该是可证明的，只有那些拐弯抹角、毫无数学含义的命题才是哥德尔所谓的那些不可证明命题。

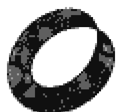
但是哥德尔并不这么认为。在1951年，他置疑我们现在的公理对于众多数论问题是否足够：

181

> 我们面对的是无穷多的公理序列，并且是可以无限延续下去，没有尽头……确实在我们今天的数学中并没有使用到那些高层次的公理……现代数学面对像黎曼假设这样的基础定理时表现出来的无能，能否利用现代数学的能力解决，我认为不太可能。

哥德尔相信，不能证明黎曼假设是因为数学本身的公理不足以解释黎曼假设。我们需要拓宽数学大厦的地基，重新构造一种数学，才能解决黎曼假设。哥德尔的不完全性定理极大地改变了人们的思维习惯。如果问题不太可能被解决，像哥德巴赫猜想或黎曼假设那样，也许它们本来就是我们使用的逻辑工具和公理无法证明的命题。

同时，我们也要谨慎，避免高估哥德尔的结果。这并不是数学的丧钟，哥德尔并没有破坏任何已经证明的结果，他的定理只是告诉我们真正的数学现实要比我们现在能用公理推导出的数学现实广泛得多。我们不断建造数学大厦的上层建筑，但同时我们也在对数学的根基进行着革命。相较于地面之上正规的建造过程，地基的革命更加依赖于数学家的直觉，来确定究竟哪一条新公理可以最好地描述数学世界。对于哥德尔的定理，许多人认为这是自从工业革命以来、思想的力量超越于机械力量的最好证明。



不可思议的思想机器

哥德尔的发现为我们提出了一个新的问题，希尔伯特和图灵对此都非常感兴趣。有没有办法来分辨真正可以证明的正确命题和那些哥德尔断言的、尽管正确但是无法证明的命题？作为一个实干主义者，图灵开始考虑是不是存在这样的机器，能够将数学家从不确定性中解救出来，避免证明一个无法证明的命题。可不可能存在这样的机器，只需要输入命题，即使无法真正地给出证明，它也能判断这个命题是否可以由给定的数学公理推出？如果是那样，它的预言，至少让我们觉得为找出像哥德巴赫猜想或黎曼假设的证明所付出的努力还是值得的。 182

这样的预言机器是否存在也是一个问题，并且这个问题还不同于希尔伯特在世纪初提出的第十问题。在第十问题中，希尔伯特猜测也许存在一个通用的算法，可以决定任何方程是否有解。希尔伯特在计算机的概念还未出现之前就已经有了这个思想，他设想存在一个机械化的过程，对于每一个方程，都能就“这个方程有解吗”这样的问题给出答案“是”或者“否”，而不需要任何操作者的干涉。

所有这些关于机器的言论都是理论上的，当时没有人能够真正制造出一台计算机。这些只是思想的机器——即产生结果的程序或算法。这说明在任何硬件出现之前，软件的思想就已经出现了。当然，即使希尔伯特的机器存在，它在现实中也毫无用处，因为利用这台机器判断任何方程是否有解所需要的时间，在很大程度上超过了宇宙的年龄。但是对希尔伯特而言，这台机器的存在与否有着哲学上的重要性。

许多数学家对这种理论机器的想法非常反感。因为这样我们就不再依赖于想象力，不再依赖人类思想的直觉来产生巧妙的论证过程，从而导致数学家失业。而取代数学家的无思想的自动机器，在面对新问题时将无法像人类那样创造出思维的新模式。哈代固执地认为这样的机器不可能存在，其观点如下：



> 当然不可能存在这样的定理，这是我们的幸运。如果存在这样的定理，说明所有的数学问题都将遵循一系列机械的规则，我们作为数学家的时代也将终结。这只是某些不懂世故的外行的想法，他们认为数学家做出发现，就像扳动某些奇妙机器上的开关那样简单。

通过一系列由剑桥大学教授马克斯·纽曼（Max Newman）于1935年春季所作的报告，图灵对哥德尔思想所包含的复杂性产生了兴趣。1928年在博洛尼亚举行了国际数学家大会，德国代表团在第一次世界大战之后首次被邀请参加会议。在这次会议上，纽曼听到了希尔伯特的报告，从此对这位伟大的哥廷根数学家的问题产生了兴趣。当时许多德国数学家拒绝参加这次会议，以抗议1924年国际数学家大会将德国代表团拒之门外。但是希尔伯特抛开这些政治分歧，带领由67名数学家组成的代表团参加了这次会议。当他走入大厅聆听开场报告时，所有的听众都站起来向他鼓掌致意。希尔伯特表达了自己的观点："认为不同的人类和种族会产生不同的科学，这是完全错误的。以此为理由的所作所为都是不公平的，数学是不分种族的……对数学而言，全世界就是一家。"

183

当纽曼在1930年听说希尔伯特的理想被哥德尔全面摧毁之后，他希望能对哥德尔的思想进行一些探索。五年之后，他觉得有了足够的信心，于是给出一系列关于哥德尔不完全性定理的报告。图灵坐在听众席中，被哥德尔证明中的迂回曲折所震撼。纽曼在结束之际给出了一个问题，在某方面我们能不能区别那些有证明的命题和那些无证明的命题？这个问题成为了希尔伯特和图灵的想象力的催化剂，希尔伯特将它命名为"判定问题（Decision Problem）"。

当他从纽曼的报告中听说哥德尔的工作之后，图灵相信不可能造出这种神奇的机器，来判定两者之间的差别。但是困难在于如何证明这样的机器不存在。毕竟，我们无法知道人类天才的局限性究竟在何处。也许可以证明某个特定的机器不可能存在，但是将这一结论推广到所有可



能的机器上，就是违反了未来的不可预见性。然而，图灵做到了这一点。

这是图灵做出的第一个大突破。他构想了一台特殊的机器，这台机器能有效地模拟人类或机器的计算过程，后来被称为图灵机。当希尔伯特构想一台能够判断命题是否可以被证明的机器时，他的概念很模糊，现在有了图灵的机器，希尔伯特的问题就成为了焦点。如果图灵的某台机器不能分辨可证明与不可证明，那么就没有其他的机器可以做到这一点。因此图灵的机器就足以解决希尔伯特的判定问题。

有一天，当图灵出去沿着卡姆河①岸跑步时，他突然想通了一个问题，为什么所有的图灵机都无法用来区分那些可证明与不可证明的命题。他停下来躺在格兰切斯特②的草场上休息，他发现曾经用来解决一个关于无理数问题的方法，可以用来解决这台验证是否可证明的机器的存在性问题。

184

图灵想到的方法来自于格奥格·康托（Georg Cantor），一位来自德国哈雷③的数学家于1873年做出的发现。康托发现存在着不同种类的无穷大。这初看起来很奇怪，但是确实是可以比较两个无穷集合，并判断哪一个大于另外一个。在19世纪70年代，康托公布了自己的发现后，这被认为是异端学说，一位疯子的胡言乱语。为了比较两个无穷大，设想有一个原始部落，他们的计数系统就是“一、二、三、许多”。即使他们无法知道准确的钱数，但是他们仍然可以判断在部落中谁是最有钱的人。如果用鸡来表示一个人的财富，那么任意两人只需要一对一对地比较各自拥有的鸡，谁的鸡不够了，就说明他的财富要比另外一个人少。他们根本就不需要知道鸡的只数，就可以比较谁更加富有。

利用这种配对比较的思想，康托表明如果你比较所有的数与所有的分数（像1/3，3/4，5/101），这两个集合的成员个数是相等的。这一点

---

① River Cam，位于英格兰中东部，长约64千米（40英里），流经剑桥。

② Granchester，英国剑桥郡的一个小村庄，在剑桥附近，以其草场闻名，是度假胜地。

③ Halle，德国中部一城市，位于萨尔河畔，莱比锡西北偏西的一座城市。



与我们的直觉相冲突，因为看上去所有的分数应该比所有的数要多出许多。然而康托找到了一个完美的配对方法，这样就不会出现分数多出来的结果。另外，康托还给出了一个漂亮的过程，证明了无法将所有的分数与实数一一匹配，实数是包括像 π 和$\sqrt{2}$这样的无理数以及具有不循环十进制展开的数。康托证明了任何试图匹配所有分数与实数的方法，都会遗漏某些具有无穷十进制展开的数。这样，我们就找到了两个无穷集合，它们的大小是不同的。

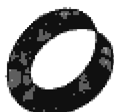
希尔伯特意识到康托正在创立一门全新的数学。他将康托关于无穷的思想描述为“数学思想产生的最令人惊讶的结果，是人类活动在纯智力领域做出的最优美结果……谁也不能将我们从康托为我们构建的天堂中赶出去。”为了突出对康托开创性工作的欣赏，希尔伯特将 23 道问题中的第一道留给了康托提出的问题：是否存在一个数的无穷集合，它大于分数集合，但是小于实数集合？

当图灵在剑桥躺着晒太阳时，闪现于他脑中的正是康托对于无穷小数多于分数的证明。他突然意识到这个思想可以用来说明，希尔伯特期望的能验证某个命题是否存在证明的机器只不过是一场空想。

185

图灵假设有一台图灵机，可以判定某个命题是否存在证明。原先，康托利用一个巧妙的思想，证明了总是有一些小数会多出来，利用同样的技巧，图灵构造出一个“多出来”的真命题，这个命题无法用图灵机来判定是否存在证明。康托方法的优美性在于，如果你试图通过修改这台机器，使得它能够适用于那条“多出来”的命题，那么总是会出现别的命题，无法用这台修改后的机器做出判断。这正如哥德尔对不完全性定理的证明一样，加入了一些公理后，总是会导致产生一些新的无法证明的命题。

图灵很清楚这样的一个证明是非常容易出差错的。当他跑回国王学院的宿舍之后，他迅速地检验这个证明，看是否存在某些漏洞。其中有一点令他很不安，他证明了不存在任何图灵机可以解决希尔伯特的判定问题，但是他怎么能说服别人不存在其他的机器可以解决希尔伯特的问



题呢？此时图灵做出了第三个突破：通用机的思想。他草拟了一台机器的蓝图，这台机器可以像任何图灵机那样运行，也可以像其他能够解决希尔伯特问题的机器那样运行。由于大脑也是一台可以判断是否可证的机器，这就激发图灵后来考虑机器是否也有思考能力这样一个问题。但是目前，他的主要精力集中在检查所有的步骤，提出希尔伯特问题的最终答案。

经过一年的辛勤工作，图灵确信自己的论证已经滴水不漏。当然他也知道，这个结果一旦宣布，将会面临最严格的审查。图灵决定，让曾经首次给自己介绍这个问题的人——纽曼——作为第一个检查者。起初，纽曼对图灵的证明感到很困惑，因为这个证明看上去似乎会误导读者将本来不正确的问题看作正确的。但是当纽曼多次阅读证明之后，他越来越相信图灵确实是解决了这个问题。然而，他们将要发现图灵并不是唯一得到这个结果的人。

186

图灵发现在最后时刻自己被一位来自普林斯顿的数学家击败。阿隆左·丘奇（Alonzo Church）与图灵几乎在同一时间得到相同的结果，但是他先于图灵将论文发表。普遍认为图灵会因为被丘奇先声夺人而失去在严酷学术丛林中的地位，但是由于得到自己在剑桥的挚友纽曼的支持，图灵的证明也得到了发表。令图灵不安的是，这份出版了的证明在当时仅仅得到了少数的认可。但是，图灵关于通用机的思想比丘奇的方法更加实用，并且有着更加广泛的影响力。图灵对现实发明的热爱也激发了他的理论思考，虽然通用机只是一个存在于思想中的机器，但是图灵对它的描述看起来更像一件实际的精密装置。他的一位朋友开玩笑说，如果这台机器真能造出来，那么一定会被放在阿尔伯特大厅①中。

通用机标志着计算机时代的到来。数学家将拥有一件强大的工具，

---

① Albert Hall，全称为 The Royal Albert Hall of Arts and Sciences 皇家阿尔伯特艺术与科学大厅。英国女皇维多利亚为了纪念自己的丈夫阿尔伯特亲王，将 1871 年落成的艺术与科学中心改名为阿尔伯特大厅。由于经常举办各种类型的音乐会，也称为皇家阿尔伯特音乐厅。



来帮助他们探索数字的宇宙。在图灵的一生中，他只能想象到真实的计算机器也许会对素数的探索有所帮助，而没能预见到自己关于机器的理论将在发现数学圣杯的过程中发挥重要作用。数十年后，一个偶然发现的公式可以生成所有的素数，而在其中，图灵关于希尔伯特判定问题极其抽象的分析成为了关键的一步。

齿轮、拨杆和润滑油

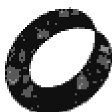
图灵的下一个任务是穿越大西洋，访问丘奇，同时他也希望能够得到认识哥德尔的机会，当时哥德尔正在普林斯顿高等研究院访问。在穿越大西洋的航程中，尽管他仍考虑理论上的机器，但他并没有失去对真实装置的热爱，在船上的一周中，他用六分仪描绘着它的草图。

当图灵到达普林斯顿的时候，他失望地发现哥德尔已经离开普林斯顿返回了奥地利。只是他不知道两年后，哥德尔为了避免欧洲的迫害活动接受了高等研究院的终身职位。图灵在普林斯顿遇到的人是哈代，哈代当时正好在那里进行访问。图灵在给母亲的信中描述了与哈代的相见："也许是因为内向，我到达的那天在毛瑞斯·普利斯（Maurice Pryce）的房间中碰到他。他一直很冷漠，都没有和我说一句话，不过现在我们的关系好多了。"

187

当图灵写出自己关于希尔伯特判定问题的证明并发表之后，他需要找到下一个进攻目标。由于希尔伯特的判定问题已足够困难，如果要选择另一个大问题，为什么不试试终极目标——黎曼假设？于是图灵让自己在剑桥的同事阿尔伯特·英格汉姆（Albert Ingham）寄来有关黎曼假设最新进展的论文，同时他也与哈代交谈，咨询哈代对这个问题的看法。

1937 年，哈代对黎曼假设的正确性更加悲观。他曾经花了那么长的时间去证明它，但换来的却是一次次失败，哈代不由得开始认为黎曼假设也许本来就是错误的。在普林斯顿的图灵受哈代情绪的影响，觉得自



己可以设计一台机器，证明黎曼假设是错误的。同时，他也听说西格尔重新发现了黎曼计算零点的绝妙方法。西格尔发现的公式巧妙地利用正弦和余弦函数的叠加估计出黎曼图像中点的高度。在剑桥，图灵攻克希尔伯特判定问题这件事被认为是对设计一台能够解决黎曼猜想的机器有很大帮助，而图灵发现这样的机器同样可以用在黎曼的秘密公式上，因为图灵知道黎曼的公式类似于某个用来预测周期物理行为（比如说行星的轨道）的公式。1936 年，牛津数学家泰德·梯奇马士（Ted Titchmarsh）利用原有的用来计算天体运行的机器，证明了 ζ 函数图像中前 1041 个零点都落在黎曼临界线上。但是图灵却见过另一台更加复杂的机器，用来计算另一种周期自然现象：潮汐。

由于涉及计算地球自身的日周期旋转、月球环绕地球的月周期旋转、以及地球环绕太阳的年周期旋转，潮汐牵涉到非常复杂的数学问题。图灵曾在利物浦见到一台能自动计算潮汐的机器，这台机器将周期正弦波的相加转变为操作一系列弦和拨杆，然后将结果用部分弦的长度表示出来。图灵写信给梯奇马士，承认自己初次见到利物浦的机器时，完全没有想到居然可以利用它来探索素数。不过现在他的思想在飞速地运行，图灵希望能够构造出一台机器，用来计算黎曼图像中的点的高度，从而期望找到一个位于海平面的点，它落在黎曼临界线之外，这样就能证明黎曼假设是错误的。

图灵并不是第一个试图利用机器来加速复杂计算的人，计算机思想的始祖是另外一位剑桥毕业生。查尔斯·巴贝奇（Charles Babbage）于 1810 年成为剑桥三一学院的学生，和图灵一样，他对于机械设备非常感兴趣。在巴贝奇的自传中，他回忆自己曾经构思一台机器用来计算数学常用表，这对于英国人在海上的航海能力非常重要：

188

> 有一天晚上，我坐在剑桥分析学会的办公室中。我趴在桌子边上，处于半梦半醒状态的时候，面前是一张对数表。一位同事走进来，见我在打瞌睡，于是叫我，“巴贝奇，你梦见了什么?”我（指着桌上的对数表）回答说，“我在思考如何利用机器来计算这些



表格。"

到了1823年，巴贝奇已经能够开始实现自己的梦想，制造一台"差分机"。但是在1933年时，由于他与主要的工程师因经费问题产生了争执，这个计划失败了。这台机器在当时只完成了一部分，直到1991年，巴贝奇诞辰200周年的时候，他的梦想才最终实现。在花费了30万英镑之后，差分机终于在伦敦的科学博物馆建成，并一直展示至今。

图灵关于ζ机的想法类似于巴贝奇利用差分机计算对数的计划，这台机器能够将复杂的问题转化为特定的可以计算的简单问题。这与图灵理论上的通用机想法完全不同，通用机可以模拟任何计算过程，而这台装置的物理特性对应于特定的问题，因此它对其他问题完全无能为力。在图灵向皇家学会申请资金建造这台ζ机的申请中，他也承认："这台机器并无太大用处……我想不出其他与ζ函数相关的应用。"

巴贝奇也意识到制造一台只能计算对数的机器是并没有太大用处。在19世纪30年代，他曾幻想制造一台更加庞大的机器，用来完成一系列的任务。当时法国人杰卡德（Jacquard）发明的卡片织布机风靡欧洲大陆，熟练的操作员只需要更换一些打孔的卡片，就可以控制织布机织出的花样。（有人认为这些卡片实际上是最早的计算机软件。）巴贝奇十分欣赏杰卡德的发明，他买了一幅有发明者画像的丝织挂毯，同样这条挂毯也是利用打孔卡片织成。"这种织布机可以织出任何人们可以想象出的图案，"巴贝奇赞叹地说道。如果像这样的机器可以织出任何图案，那为什么不可以制造一台机器，通过输入卡片，让它进行不同的数学计算？他将这种机器命名为分析机（Analytical Engine），分析机就是图灵通用机的祖先。

189

诗人拜伦爵士（Lord Byron）的女儿，阿达·拉夫拉斯（Ada Lovelace）认识到巴贝奇机器的巨大潜力。在将巴贝奇关于机器的论文翻译成法文的时候，她忍不住在旁边加上了一些赞扬机器能力的评注，"最恰当的比喻就是，分析机织出的是代数图案，而杰卡德的织布机织出的是花朵和绿叶。"她的评注还包括了许多可以利用巴贝奇的机器实现的



程序。当她完成翻译的时候，她的评注已经很多，以至于法文版的长度是英文版的3倍。现在拉夫拉斯被公认为世界上最早的计算机程序员，她于1852年死于癌症的痛苦中，年仅36岁。

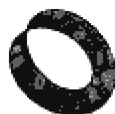
当巴贝奇在英国辛勤地为自己梦想中的机器奋斗时，黎曼正在德国发展着自己的理论数学概念。80年后，图灵希望将这两者结合到一起。他已经在哥德尔不完全性定理的抽象计算性上小试牛刀，这是他博士论文的主要部分。现在他希望在由齿轮组成的ζ机方面崭露锋芒。由于哈代和梯奇马士的支持，图灵成功地从皇家学会得到了40英镑的赞助。

据图灵传记的作者安德鲁·霍奇斯（Andrew Hodges）的描述，到了1939年夏天，图灵的房间中“乱七八糟的齿轮铺满了一地”。但是图灵关于ζ机的梦想，以及将19世纪英国人对机器的热情和德国人的理论结合起来的工作，正处于即将陷入中断的危机之中。第二次世界大战的爆发，使得两个国家之间刚建立不久的学术交流变成了军事冲突。英国的知识分子被集中到了布莱切利庄园，目标也由寻找零点变成了破解密码。利用平时积累的计算黎曼ζ函数零点的技术，图灵成功地设计了一台机器，用来破解Enigma密码。图灵设计的复杂联锁齿轮装置还没有发现素数的秘密，但是却被成功地用来破解了德国战车的秘密移动信息。

190

布莱切利庄园是象牙塔和现实世界的奇妙混合体，它像剑桥大学一样，有草地可以进行板球活动。对图灵和同事而言，在这个隐蔽的乡下，每天送过来的加密信息，就如同在剑桥休息室中进行的时代杂志上的填字游戏。虽然是理论谜题，但他们知道有许多生命依赖着自己的结果。在这样的气氛下，图灵在帮助赢得战争的同时，也需要不断地思考数学问题。

正是在布莱切利，图灵开始理解为什么建造一台可以按照指令进行不同任务的机器，要比针对不同问题建造一台全新机器更好，这也是100年之前巴贝奇的想法。虽然图灵已经从原理上意识到这一点，但他也知道要将它变成现实将是一段艰苦的路程。当德国人改变了战争中所



用 Enigma 机器的设计之后，布莱切利庄园陷入了数周的低潮。图灵意识到密码破译员需要一台机器，能够适应德国人对他们的密码机所做的任何改动。

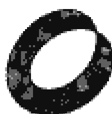
在战争结束后，图灵开始考虑建造一台通用计算机器的可能性，这台机器应该可以在程序的指挥下执行一系列的任务。经过 7 年在英国国家物理实验室（Britain's National Physics Laboratory）的工作，图灵来到曼彻斯特新建造的皇家学会计算实验室（Royal Society Computing Laboratory）与纽曼一起工作。纽曼曾经在剑桥陪伴图灵设计了一台理论机器，摧毁了希尔伯特关于是否存在一个算法，可以判定一个真命题是否存在证明的梦想。现在他们又走到了一起，合作设计并建造一台真正的计算机器。

在曼彻斯特，图灵有了充分的时间考虑自己在布莱切利庄园设计的机器的技术原理，尽管那台机器以及图灵战时的活动在数十年内都被列为最高机密档案。他又重新开始考虑战前那个曾经吸引过自己的问题：利用机器探索黎曼的图像，找到一个落在临界线之外的零点，从而推翻黎曼假设。但是这次，图灵并非打算建造一台机器，其物理性质对应于所要求解的问题；而是试图写出一段程序，可以在他和纽曼利用电子管和磁鼓建造的通用机器上运行。

当然，理论机器可以毫不费力地平稳运行，但是实际机器，就像图灵在布莱切利发现的那样，并不是十分可靠。到了 1950 年，图灵的新机器已经建造成功，可以开始在 ζ 函数图像中进行探索了。战前的有关零点的纪录由哈代的学生梯奇马士保持，梯奇马士验证了最初 1041 个位于海平面的零点都满足黎曼假设。图灵希望可以走得更远，用自己的机器检查前 1104 个零点，但是他写道，“不幸的是，在接近结束的时候，机器崩溃了。”而这并非是第一次的机器崩溃。

191

此时，图灵的个人生活也开始陷入低潮。1952 年，他因为同性恋倾向被警察逮捕。他因为失窃叫来了警察，而这位窃贼认识图灵的某位同性恋人。在追踪窃贼的过程中，图灵向警察承认，承认自己犯有（当时



法律所称的）“下流的行为”。图灵因此心烦意乱，因为这意味着即将面对牢狱之灾。纽曼则辩称图灵是“完全沉溺于工作之中，并且是同时代最有创造力和想象力的数学家”。图灵逃过了坐牢的惩罚，但条件是自愿接受药物治疗，控制自己的性取向。图灵给自己在剑桥的老师写信说，“有人说它（药物）是用来控制性欲，也有人说停用它之后又会恢复原状，我希望他们说的是正确的。”

1954 年 6 月 8 日，图灵因氰化物中毒死在家中。图灵的母亲不能接受图灵自杀的解释，因为她的儿子从小就进行许多化学实验，并且从来不洗手。她认为这是一起意外事故，在图灵的床边有一个被咬了几口的苹果，虽然这个苹果并没有经过检验，但还是有人怀疑这个苹果曾沾上了氰化物。图灵最喜欢的电影场景就是迪斯尼的《白雪公主与七个小矮人》中，继母利用了一个可以令白雪公主沉睡的苹果：“毒液浸透苹果，如睡之死渗人。”

在图灵逝世 46 年之后的新世纪到来之际，数学圈中有人开始传说，其实图灵的机器找出了黎曼假设的一个反例，但是由于这个发现是在第二次世界大战时期的布莱切利庄园用破解 Enigma 密码的同一台机器做出的，英国情报机构必须将它置于严格保密之下。因此数学家强烈要求解密战时的档案，以寻找那个不在临界线上的零点。最后事实证明，这个谣言来自于邦比艾里的朋友，与这位意大利数学家一样，他只不过是开了一个愚人节的玩笑。

192

只不过是对于战前纪录的小小突破，就让图灵的机器崩溃。但这却宣告了一个时代的到来，计算机可以取代人脑进行对黎曼图像的探索。只需假以时日，就能制造出高效的“黎曼图像漫游者”，这个非人类的探索者可以在黎曼的临界线上越走越远，并反馈回越来越多的证据——如果没有最终的证明——说明事实正好与图灵的直觉相反，黎曼假设是正确的。

虽然图灵的真实机器对黎曼假设产生了一定的影响，但是他的理论思想却为素数故事带来一个奇妙的结果：能够生成所有素数的公式。图



灵肯定从未想过，这个公式会在他和哥德尔所摧毁的、希尔伯特所希望的数学的坚实基础的废墟上，得到新的生命。

从不确定性混沌到素数公式

图灵已经证明，他的通用机也不能回答数学中的所有问题。但是如果我们降低要求，只考虑方程是否存在解的问题，那么通用机是否可以给出一个答案？这正是希尔伯特第十问题的核心所在。1948 年，伯克利的天才数学家朱莉亚·罗宾逊（Julia Robinson）开始考虑这个问题。

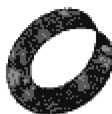
直到最近几十年，除了非常著名的那几位女数学家，数学史中几乎没有太多女性的存在。曾经与高斯通信的法国数学家索菲·热尔曼（Sophie Germain）在信中装成一位男性，因为她害怕暴露自己女性身份之后，自己的思想会被别人置之一旁。她曾发现某些与费马大定理有联系的特殊素数，这些素数现在被称为热尔曼素数。高斯收到这位“布朗克先生”的信件之后，对他留下了深刻的印象。当高斯在一段时间通信之后发现这位先生其实是位女士的时候，他更加惊讶，在回信中他这样写道：

> 数的神秘性是如此地不同寻常……这门卓越学科的魅力与美只向那些有勇气探索的人展现。但是当一位女性，由于她的性别、我们的传统以及偏见……克服了这些禁锢，看出了隐藏之中的秘密。她毫无疑问有着非凡的勇气、超常的天赋以及出众的能力。

193

高斯曾要求哥廷根授予热尔曼荣誉学位，但是热尔曼在此之前就离开了人世。

在希尔伯特时代的哥廷根，艾米·诺特（Emmy Noether）是一位非常有才华的代数学家。希尔伯特曾为了她挑战德国学术机构中女性无法取得职位的传统。希尔伯特说，大学并非公共浴室，因此“我认为候选人的性别不应该成为阻止她加入的理由。”由于诺特是犹太人，最后也



不得不逃离德国去了美国。后来数学中某个特定的代数结构就以诺特命名。

朱莉亚·罗宾逊并不仅仅是一位天才的数学家，她也是一位60年代的女性，她的成功激励更多的女性投身数学事业。由于她是学术界中仅有的几位著名女性，她后来回忆为什么经常被要求参加某些调查，"只要科学地选择样本，其中一定会有我。"

罗宾逊的童年在亚利桑那州的沙漠地区度过，与妹妹和土地做伴的生活十分的孤独。在她很小的时候，她已经能够发现隐藏在沙漠中的图案。她回忆说，"我最早的记忆是在巨大的仙人掌阴影中排列鹅卵石。由于阳光十分强烈，我只能半眯着眼睛看这些图像。我觉得我对自然数有一种天生的热爱，对我而言它们是唯一真实的东西。"在她9岁的时候，她患上了风湿热，并因此卧床好几年。

这样的一种孤独生活往往是年轻科学家的灵感来源。柯西和黎曼都曾经因为现实世界中精神和肉体的问题而逃避到数学世界中去。虽然罗宾逊卧病在床的时候没有发现什么定理，但是她学习了许多技巧，为将来面对数学问题打下了相当的基础。"我认为在那几年病床上的岁月中，我学会了顽强，我的妈妈说我是她见过的最顽强的儿童。我必须说正是我的顽强，才能让我在数学中取得成功。而顽强是所有数学家共有的特性。"

等到罗宾逊恢复健康，她已经错过了两年的学习。然而经过一年的家庭学习，她发现自己已经走到了同学的前面。有一次，她的老师在课堂上讲到，古希腊人在2000多年之前已经知道2的平方根无法用分数准确表示。不像分数的十进制小数展开，2的平方根的十进制展开不会出现循环现象。对罗宾逊而言，证明这个结果是非常奇妙的一件事，怎么知道在小数点后100万位也不会出现某些规律呢？"我回到家之后，利用我刚学会的求平方根的方法来检验这个结果，最终我在傍晚的时候放弃了。"有了这次失败，罗宾逊开始认识到数学语言的能量。因为它能让你确信，无论计算到小数点之后多少位，2的平方根的十进制展开

194



永远不会出现循环。

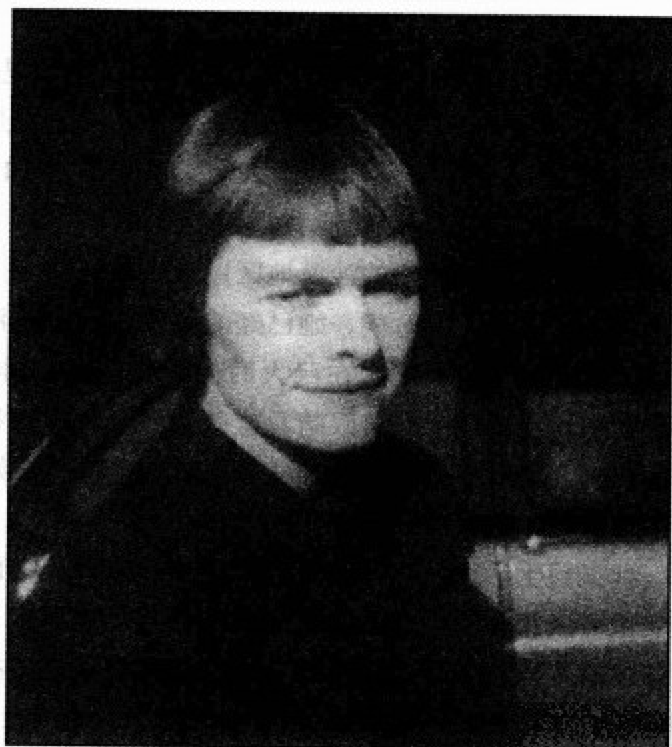


图 32 朱莉亚·罗宾逊，1919～1985

正是这种简单论证的能力吸引许多人投身数学世界。这个问题是无法用蛮力计算出来的，即使有最强大计算机的帮助也无法解决。但是将一些精心挑选的数学思想组合在一起，就可以揭露无穷十进制展开的奥秘。不必去做检查无穷位小数这样的不可能任务，只需经过简单论证即可完成这项任务。

当罗宾逊 14 岁时，她已经不满足于学校里乏味的算术课程，开始寻找其他的数学资源。她很喜欢听一个叫做“大学探索者”的广播节目，其中有一集关于数学家德里克·诺曼·莱默（Derrick Norman Lehmer）和他儿子德里克·亨利·莱默（Derrick Henry Lehmer）的故事特别吸引罗宾逊。广播中详细介绍了这些数学家如何利用自行车的齿轮和



链条，制造计算机器来攻克数学问题的故事。小莱默是从图灵手中接过接力棒的人，在1956年他利用现代计算机证明了前25000个零点都满足黎曼假设。老莱默则描述他们战前的机器“在幸福地运行了几分钟后突然卡壳，然后又接着运行，又再次卡壳”。最后他们找到了出问题的原因：一位邻居正在听收音机。父子俩最关心的数学问题就是找出大整数的素数因子。罗宾逊对节目中描述的机器十分感兴趣，她还因此写信去索取这次广播的文字稿。

罗宾逊在报纸上发现了一篇关于发现素数的报道，于是她将其剪了下来。在这篇题为“寻找最大素数事件无人关注”的报道中，记者写道：

> 萨缪尔·I·克雷格（Samuel I. Krieger）博士在用去六枝铅笔、七十二张标准纸，耗费无数精神之后，终于在今天宣布231 584 178 474 632 390 847 141 970 017 375 815 706 539 969 331 281 128 078 915 826 259 279 871是目前已知最大的素数。但是他不愿意说谁会关注这个结果。

也许无人关注的现象反映了一个事实，这个数实际上可以被47整除（如果编辑验证过这个数，当时就应该知道这个结果）。罗宾逊一生都带着这份剪报和关于莱默计算机器的广播稿，以及一本关于第四维神秘性的小册子。

罗宾逊数学生涯的地基已经打牢。她在圣地亚哥州立学院①获得数学学位，然后去加州大学伯克利分校进行深造。那里的一位教师拉非尔·罗宾逊（Raphael Robinson）不光激发了罗宾逊对数论的兴趣，后来还成为了她的丈夫。当他们还在交往的时候，拉非尔就发现数学可以打动朱莉亚的心，于是他开始向她介绍最新的数学发展。

拉非尔谈到的关于哥德尔和图灵的成就，引起了朱莉亚格外的关

① San Diego State College，现为圣地亚哥州立大学。



注。“有关数的结果竟然能通过符号逻辑得到证明，这令我十分震惊和兴奋，”朱莉亚说。抛开哥德尔结果中令人不安的部分，她对小时候在沙漠中玩耍鹅卵石得到的关于数的真实性的感觉仍然很强烈，“我们可以想象一种完全不同于现在的化学或者生物学，但是我们不能想象另外一种关于数的数学。一旦得到证明，这些关于数的结论应该是在任何宇宙都通用的。”

196

虽然罗宾逊拥有非凡的数学能力，但她也承认没有自己丈夫的支持，她在做数学的时候便不会如此轻松。在当时女性几乎很难维持自己的学术生涯，伯克利的大学规定夫妇俩人不能在同一系任教，但由于罗宾逊的研究能力非常出众，统计学系为她提供了一个职位。她随职位申请书一同交给人事部门的工作描述，是典型的数学家的一周工作情况："周一：试图证明定理；周二：试图证明定理；周三：试图证明定理；周四：试图证明定理；周五：定理错误。”

当罗宾逊得到一个向20世纪最著名的逻辑学家学习的机会之后，她对哥德尔和图灵工作的兴趣被充分地激发出来。波兰人阿尔弗莱德·塔斯基（Alfred Tarski）在1939年访问哈佛大学时，由于家乡爆发了战争而留在了美国。由于罗宾逊不想放弃自己对数论方面的热情，于是她的目标就是代表两个领域完美组合的希尔伯特第十问题：是否存在一个算法——以计算机的语言来说，就是一个程序——可以用来判断给定的方程是否有解？

根据哥德尔和图灵的结果，我们清楚地知道，与希尔伯特的意愿相反，这样的程序可能不存在。不过罗宾逊确信可以有方法来利用图灵已经得到的结果，她知道每个图灵机都会产生一串数，比如说，某个图灵机可以产生一系列的平方数1，4，9，16，…而另外一台图灵机则产生素数。图灵关于希尔伯特判定问题的结果之一是证明了给定一台图灵机和一个数，能够判断可以由这台图灵机产生这个数的程序是否存在。于是罗宾逊试图寻找图灵机和方程之间的联系。她相信，每个图灵机都对应着一个特殊的方程。



如果存在着这样的联系，罗宾逊希望知道，判断一个数是否可以由一台图灵机产生的问题，是不是就转化为对应于这台图灵机的方程是否有解的问题。因此，如果她能够建立这样的联系，她就能成功。如果像希尔伯特提出第十问题时所想的那样，存在着一个程序可以判断方程是否有解，那么通过罗宾逊建立的方程与图灵机之间（仍是设想中）的联系，就可以利用整个程序来检验那个数是否是图灵机的输出数。但是图灵已经证明了这样的程序——可以用来决定图灵机输出的程序——不存在，因此判断方程有解的程序同样不存在。所以希尔伯特第十问题的答案是“不存在”。

罗宾逊开始思考为什么每个图灵机都会有对应的方程。她想找到一个方程，其解恰好与图灵机输出的一列数存在着联系。她觉得向自己提出这样一个问题令自己相当兴奋，“通常在数学中给定一个方程，你总是试图去寻找解；现在给你一个解，要找出原来的方程。我喜欢这样的问题。”在1948年，罗宾逊对这个问题的兴趣愈发强烈。因为在她9岁的那场大病之后，医生曾预言由于她的心脏很虚弱，她不会活过40岁。每年的生日，“我总是在吹灭蛋糕上的蜡烛的时候，暗暗许下诺言，希望第十问题可以解决——并不一定是由我解决，仅仅是希望它能够得到解决，因为我不能忍受在没有结果的情况之下离开这个世界。”

一年年过去，罗宾逊也做出越来越多的结果。有两位数学家加入了她的工作，马丁·戴维斯（Martin Davis）和希拉里·普特南（Hilary Putnam）。到了20世纪60年代末期，他们已经将这个问题归化为更简单的问题。他们发现，不用去找到满足图灵机输出结果的所有方程，只需要找到一个方程，满足一列特殊的输出数，他们就可以证明罗宾逊的猜测。这是十分了不起的发现，所有的工作就是寻找满足这一列数的方程。对于他们构建的数学墙而言，整个理论完全依赖于是否能够证实其中一块砖头的存在性。如果事实证明这一列数不存在所谓的罗宾逊方程，那么他们耗费这么长时间建造起来的数学之墙将在瞬间崩塌。

有人怀疑罗宾逊的方法并不是攻克希尔伯特第十问题的正确方法，



一些数学家抱怨这只会将人引入歧途。就在这时，1970 年 2 月 15 日，罗宾逊接到一位刚从西伯利亚会议回来的同事的电话，他说在这次会议上出现了一个非常有趣的结果，也许罗宾逊会有兴趣。一位 22 岁的俄罗斯数学家尤里·马迪亚塞维奇（Yuri Matijasevich）发现了拼图的最后一块，从而解决了希尔伯特第十问题。他证明了存在一个方程，可以产生罗宾逊预言的那一列数。这正是罗宾逊整个方法所依赖的那块砖头。希尔伯特第十问题也因此得到了完满解答：能够判定某个方程是否有解的程序不存在。

198

“那一年，当我想再次吹灭蛋糕上的蜡烛时，突然意识到那个我许了多年的愿望已经实现了。”罗宾逊知道结果其实一直就在自己的眼皮底下，只不过是马迪亚塞维奇发现了它。“有许多东西，一直就藏在沙滩底下，只是我们无法看到而已。直到某天有人将它们捡起，那时所有人都看见了，”罗宾逊这样说道。她给马迪亚塞维奇寄去祝贺的信件：“我一直在想，当我第一次提出这个猜想的时候你还是个婴儿，我所能做的事就是等待你长大。”

数学能够穿越政治和历史的边界线，将人们团结在一起。抛开冷战时期不同的意识形态，美国和前苏联的数学家为了希尔伯特问题建立了强大的友谊。罗宾逊描述了数学家之间这种奇怪的纽带就像“没有地理起源、人种、族群、性别、年龄甚至是时间差别（过去和将来的数学家都是我们的同事）的联盟——所有人都献身于艺术和科学中最美丽的学科”。

马迪亚塞维奇和罗宾逊为证明的归属问题产生了争论，只不过并不是为了自己的名誉——他们都坚称是对方做出了最关键的一步。一般而言，由于马迪亚塞维奇找到了拼图的最后一块，完成了证明，因此希尔伯特第十问题的解决通常被认为是他的成果。事实上，在希尔伯特于 1900 年提出问题以来，70 年中有许多数学家都为这段漫长的历程做出了贡献。

尽管这个问题被否定了，即不存在一个程序可以用来判定是否任意



方程都有解——但是数学家并非一无所得。罗宾逊相信，某一列由图灵机生成的数可以用方程来描述。这一点已经得到了证明，同时数学家也知道有一台图灵机可以生成所有的素数。因此，多亏了罗宾逊和马迪亚塞维奇的工作，我们知道在理论上存在着一个公式可以生成所有的素数。

但是数学家能找到这个公式吗？1971 年，马迪亚塞维奇找到一种直接的方法，可以用来得到这个公式，但是他并没有接着做下去得到答案。在 1976 年，人们找到第一个详细的精确公式，它涉及到 26 个变量，从 A 到 Z：

199

$$
\begin{aligned}
&(K+2)\{1-[WZ+H+J-Q]^2-[(GK+2G+K+I)(H+J)+H\\
&-Z]^2-[2N+P+Q+Z-E]^2-[16(K+1)^3(K+2)(N+1)^2+1\\
&-F^2]^2-[E^3(E+2)(A+1)^2+1-O^2]^2-[(A^2-1)Y^2+1-X^2]^2\\
&-[16R^2Y^4(A^2-1)+1-U^2]^2-[((A+U^2(U^2-A))^2-1)\\
&\times(N+4DY)^2+1-(X+CU)^2]^2-[N+L+V-Y]^2\\
&-[(A^2-1)L^2+1-M^2]^2-[AI+K+1-L-I]^2\\
&-[P+L(A-N-1)+B(2AN+2A-N^2-2N-2)-M^2]^2\\
&-[Q+Y(A-P-1)+S(2AP+2A-P^2-2P-2)-X]^2\\
&-[Z+PL(A-P)+T(2AP-P^2-1)-PM]^2\}
\end{aligned}
$$

这个公式就像计算机程序，只要随机地改变 A 到 Z 的取值，比如说取 $A=1$，$B=2$，…，$Z=26$ 代入这个公式进行计算，如果输出的结果大于零，那么这个结果一定是素数。你可以重复这个过程，选取不同的数值代入符号 $A\cdots Z$ 并进行计算。在你为 $A\cdots Z$ 取遍所有可能的数值之后，可以保证这个公式能够得到所有的素数。不用担心会有素数丢失，因为总存在某种选择方法，使得这个公式输出你所需要的素数。但是这里仍然有一些小问题，为 $A\cdots Z$ 选择某些数的时候，结果会出现负数，这时我们只需将其忽略。就像上面我们选择 $A=1$，$B=2$，…，$Z=26$，此时的结果为负数，因此我们就将它省略。

这是不是就是我们寻找的圣杯——这个不同寻常的能够生成所有素



数的多项式？如果这个公式能够在欧拉那个年代被发现，这将成为当时最轰动的新闻。欧拉发现了一个公式，它能生成许多素数，但是是否能发现一个可以生成所有素数的公式，欧拉对此持有悲观的态度。但是到了现在，数学家已经从仅仅是研究方程和公式，转变为接受黎曼的信仰，开始研究数学世界内部的根本结构和主题，数学探索者们都在忙于描绘通往新世界的航线，因此这样的素数公式只能说出现的不是时候。对新一代的数学家而言，这样的公式类似于多年前的技术型探索，因此不值得重视。但是，数学家仍然对存在这样一个公式感到惊讶，只是黎曼已经将素数的研究带领到另外一片新天地中。在柴可夫斯基的时代谱写并演奏莫扎特风格的交响曲，根本就不能打动观众，即使有人会关注它形式上的完美。

200

然而，并非是这种新的数学审美观影响了学术界对这个神奇公式的承认。事实是，这个公式没有任何实际用途，因为大部分的输出值都是负数。同时它在理论上也缺乏重要意义，罗宾逊和马迪亚塞维奇证明了，由图灵机产生的任意一列数都存在像这样的公式，在这个意义上，素数序列相比较于其他数的序列没有任何特殊性。同样这也是大多数人的观点，当某人告诉俄罗斯数学家林尼克(Yu. V. Linnik)马迪亚塞维奇关于素数的结果时，他回答说，"太好了，这样我们就有可能知道素数的一些新性质了。"但是当他知道这个结果是如何被证明，以及可被用于任意一列数的时候，林尼克收回了起初的欣喜，"真可惜，这样我们就没有可能知道素数的一些新性质了。"

如果对于任意数的序列，都存在这样的一个公式，那么这个素数公式就无法告诉我们任何新东西。这也就说明了黎曼对于素数的处理更加有意义。黎曼图像的存在，以及他为每一个海平面上的点赋予的音符，对于素数而言都是完全唯一的。在其他任何一列数中都不会存在如此和谐的结构。

当罗宾逊解决了希尔伯特第十问题的时候，她在斯坦福的一位朋友也摧毁了希尔伯特的另外一条信仰，希尔伯特曾认为在数学中没有东西



是不可知的。1962年，还是学生的保罗·科恩(Paul Cohen)就自信地问斯坦福的教授，解决希尔伯特的哪一条问题可以使自己出名。他们想了一下，告诉科恩希尔伯特第一问题是最重要的。粗略地讲，就是问自然界中有多少个数。作为一系列问题中的第一个，希尔伯特选择了康托关于不同等级无穷大的问题。是否存在着一个由无穷多个数组成的集合，它大于分数集合，但是又比所有实数的集合小，这里实数是指包含像 π、$\sqrt{2}$ 那样的无理数，或是那些有无穷十进制展开的数。

当科恩于一年之后回来的时候，希尔伯特在坟墓中也应该惊讶地坐起来。他带回的答案告诉我们：两种结果都有可能！科恩证明了这样一个最基本的问题恰好就是哥德尔所谓的一个无法证明的命题。因此，并非只有模棱两可的命题是不可证明的。科恩实际上是证明了：在我们用来构建数学的基本公理之上，无法证明存在这样一个集合，它的大小严格地介于分数集合与实数集合之间；同时，我们也无法证明不存在这样的集合。科恩实际上是在我们现有的数学公理之上，构造了两种不同的数学世界。在其中一个世界中，康托问题的答案是“存在”；而在另外一个世界中，康托问题的答案是“不存在”。

有些人认为科恩的结果可以和高斯的发现相比较。高斯当年曾意识到除了我们身处的物理世界的几何之外，还存在着其他不同的几何。在某种意义上，两者确实很相似。但是，数学家对于数所代表的意义有着很强的直觉，他们认为，这些用来证明关于数的性质的公理也应该适用于那些“超自然”的数。不管怎样，大部分数学家还是认为康托问题对于我们构建数学大厦的数而言是正确的。罗宾逊将这些大部分数学家对科恩证明的意见搜集起来，写信给科恩说，“上帝知道，只有一种真实的数论，这就是我的信仰！”但是在寄给科恩之前，她划去了最后一句。

科恩奠基性的工作，虽然扰乱了数学的正统观念，但还是为他赢得了一枚菲尔兹奖牌。在他做出了这项惊人的成就，证明了我们不能从经典的数学公理出发决定康托问题的答案之后，科恩决定转向他认为是下一个富有挑战性的希尔伯特问题：黎曼假设。科恩是少数承认曾在这道著



名问题上下过苦功的数学家，但是科恩的进攻对黎曼假设没有任何效果。

有趣的是，黎曼假设与康托问题完全不是一个类型。如果科恩同样成功地证明黎曼假设在现有数学公理体系中也是不可判定的，那么实际上他就证明了黎曼假设是正确的！如果黎曼假设是不可判定的，这就意味着或者它是错误的，但我们不能证明；或者它是正确的，但我们同样不能证明。如果黎曼假设是错误的，就说明存在一个零点落在临界线之外，我们可以用它来证明黎曼假设是错误的。如果我们不能证明它是错误的，它就不可能是错误的。因此黎曼假设不可判定的唯一结果就是，它是正确的，只是我们还无法找到一个证明，证明所有的零点都落在临界线上。图灵是首先发现黎曼假设这一奇怪断言的人，但是很少有人相信这种逻辑学上的花招可以用来成功解决希尔伯特第八问题。

感谢图灵的通用机思想，这种思想的机器在我们理解数学世界的过程中发挥了重要的作用。但是在 20 世纪后半叶兴起的却是图灵试图制造的现实机器，由电子管、电线和硅组成的，而非神经元和无穷记忆体组成的计算机构成了这次浪潮的主体。在全世界的范围内，这些机器不断地被制造出来，帮助数学家探测更深的宇宙世界。

202

203



第九章

计算机时代:从头脑到台式计算机

我敢打赌,证明黎曼假设将不需要计算机。

——吉拉德·福瑞(Gerhard Frey),

费马大定理与椭圆曲线之间关键联系的发现者

一旦离开了学校,大部分人单独碰到素数的机会基本上是通过新闻中关于大型计算机发现最大已知素数的报道。朱莉亚·罗宾逊珍藏的剪报《发现最大素数》就说明在 20 世纪 30 年代,即使是不正确的发现也能成为新闻。多亏了欧几里得证明了存在着无穷多个素数,这样的新闻故事才可以永远地进行下去。到了第二次世界大战结束之际,已知最大的素数有 39 位,它从 1876 年被发现以来一直保持这个纪录。今天,最大素数的纪录已经超过了 100 万位,这样的数打印出来要比这本书厚出许多,将它读完则需要 1 个月。正是计算机让我们达到了这种高度,在布莱切利,图灵已经考虑过如何利用他的机器来发现破纪录的素数。

虽然图灵理论上的通用机可以拥有无穷大的内存来存储信息,但是他和纽曼在曼彻斯特建造的机器只能存储非常有限的内容,这台机器只能进行不需要太多内存地计算。比如说,生成斐波纳契数列(1,1,2,3,5,8,13,…)时只需要记住序列中的前两个数,因此他们的机器可以毫不费力地计算出这个序列。当时图灵还知道一个聪明的技巧,这是莱默家族中一位年轻成员发明的方法,可以用来找出 17 世纪修士梅森提出的特殊素数。图灵意识到,和斐波纳契数列一样,莱默的检验方法不需要太多内存,搜寻梅森素数就是图灵机器刚好可以胜任的最好工作。



梅森偶然发现,可以通过将 2 自乘若干次之后减去 1 得到素数。比如说,$2\times2\times2-1=7$ 就是素数。他还发现,如果想要 2^n-1 成为素数,数 n 必须为素数。然而即使这样,也不能保证 2^n-1 一定为素数。虽然 11 是素数,但 $2^{11}-1$ 就不是素数。梅森做出预测:

204

2,3,5,7,13,19,31,67,127,257

是 257 之内能使得 2^n-1 为素数的所有数。

像 $2^{257}-1$ 这样的数是如此巨大,仅凭人类的大脑几乎不可能检验它是否为素数。这也许就是梅森如此自信做出这样的预测的原因,他相信"所有的时间都不够用来检验这些数是否为素数"。梅森素数选择的依据是欧几里得关于无穷多素数的证明,取一个像 2^n 这样能被许多数整除的数,然后再减去 1 就可以使得它不可分解。

尽管这样并不能保证可以得到素数,但是从某方面看梅森关于数的直觉还是正确的。因为梅森数很接近于高度可分数 2^n,因此有一个很有效的方法来判断梅森数是否为素数。这个方法由法国数学家爱德华·卢卡斯(Édouard Lucas)于 1876 年发明,并因此证实了梅森数 $2^{127}-1$ 为素数。这个 39 位的素数一直保持最大素数的纪录直到计算机时代的来临。利用自己的新方法,卢卡斯成功地揭示了梅森素数表的秘密,这位修士列出的使得 2^n-1 为素数的数 n 的名单并非完全正确:他漏掉了 61,89 和 107,多加了 67。但是 $2^{257}-1$ 是否为素数,卢卡斯也无能为力。

梅森神秘的直觉被认为是盲目的猜测,他的名声也许受到了影响,但是他的名字却作为大素数之王永远流传。成为新闻的、破纪录的大素数无一例外都是不可分的梅森数。虽然卢卡斯证实了 $2^{67}-1$ 不是素数,但是他的方法却不能找出这个合数的素因子。正如我们即将看到的,分解这样的数被认为是极其困难的问题,因此也成为现今加密安全系统的核心,也是图灵在布莱切利破解的 Enigma 密码系统的继任者。

图灵并不是唯一思考过素数与计算机关系的人。正如童年罗宾逊在收音机中听到的那样,莱默家族已经有了用机器探索素数的思想。老莱默在 20 世纪初的时候已经编制出了直到 10 017 000 的素数表。(从那以



后没有人出版过更大的素数表。)他的儿子则在理论上做出重要贡献,1930年,小莱默改进了卢卡斯的检验方法,可以更有效地检验一个梅森数是否为素数。

205

为了证明一个梅森数是素数,也就是证明它不能被任意更小的数整除。当 2^n-1 可以整除一个叫做卢卡斯-莱默数的时候,可以证明 2^n-1 是素数。卢卡斯-莱默数记为 L_n,它们像斐波纳契数列那样,由数列中的前项生成,为了得到 L_n,你需要将前一项 L_{n-1} 平方,然后减去2:

$$L_n=(L_{n-1})^2-2$$

这个检验从 $n=3$ 开始,对应的卢卡斯-莱默数就是 $L_3=14$,由此我们可以得到 $L_4=194$ 和 $L_5=37634$。检验的威力在于,你只需要生成相应的 L_n,然后判断梅森数 2^n-1 是否可以整除这样的 L_n 就可以,这就是简单的验算。比如说,由于 $2^5-1=31$,它能整除相应的卢卡斯-莱默数 $L_5=37634$,因此梅森数 2^5-1 就是素数。利用这个结果,小莱默解决了梅森素数表中的最后一个数,他证明了梅森是错的,$2^{257}-1$ 并非素数。

卢卡斯和莱默是如何发现检验梅森素数的方法?这并不是一件很容易想到的事。这样的发现与黎曼假设的发现,或者高斯关于素数与对数之间联系的发现完全不同。卢卡斯-莱默检验并不是能够通过实验或数值观察能够得出的结论,他们能得出这样的结果,在于他们对于 2^n-1 是否为素数这一命题的不断探索。就像魔方那样翻来覆去的尝试,突然发现有一种方法,可以让相同的色块转到同一面。每一步尝试就如同证明中的一步,和其他具有明确目标的定理不一样,卢卡斯-莱默检验完全是在没有方向的情况下出现的结果。卢卡斯最先开始转动这个魔方,而莱默则成功地将它转化为现在一直在使用的简单形式。

当图灵在布莱切利破解德国 Enigma 密码的时候,他曾和同事讨论过,利用类似于"炸弹"这样的机器在寻找大素数方面的潜力。由于有了卢卡斯和莱默的方法,梅森数就成为他们首先需要检验的对象。这个方法特别适合于计算机进行自动计算,但是战争的压力使得图灵没有机会实现自己的想法。在战后,图灵和纽曼开始继续这项工作,寻找更多

206 的梅森素数，同时这也是对他们在曼彻斯特实验室中建造的机器的最好测试。因此虽然他们的机器只有很小的存储空间，但卢卡斯-莱默检验不需要太多的内存，为了计算第 n 个卢卡斯-莱默数，计算机只需要记住第 $n-1$ 个数就可以了。

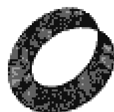
图灵曾在寻找黎曼零点的工作中失败，这次在寻找梅森素数的过程中，好运也并没有降临。他在曼彻斯特的计算机没能超过那个已经保持了 70 年的纪录 $2^{127}-1$，因为现在知道下一个梅森素数应该是 $2^{521}-1$，这在当时已经远远超出图灵机器的极限了。命运就是如此的奇妙，是罗宾逊的丈夫拉非尔·罗宾逊发现了下一个大素数。他偶然得到了一份小莱默在洛杉矶建造的一台计算机的操作手册，当时小莱默已经不再像战前那样，使用齿轮和链条建造计算机，他是国家标准局[①]数值分析研究所的负责人，小莱默建造了一台计算机叫做标准西部自动计算机（Standards Western Automatic Computer，SWAC）。从未见过计算机的拉非尔·罗宾逊在伯克利同事的帮助之下，写了一个程序，可以在 SWAC 上运行并寻找梅森素数。在 1952 年 1 月 30 日，计算机发现了第一个在人类计算极限之外的素数，仅仅在找出 $2^{521}-1$ 这个破纪录的素数之后几小时，SWAC 又发现了另外一个更大的素数 $2^{607}-1$。在这一年中，拉非尔·罗宾逊又三次打破自己保持的纪录，至此最大的素数是 $2^{2281}-1$。

搜寻新素数的竞赛，其实是掌握在那些可以接触到强大计算机的人手里。到了 20 世纪 90 年代中期，新的纪录是由计算机世界的巨人克瑞（Cray）计算机保持。成立于 1971 年的克瑞研究所，发现计算机并不需要结束上一个操作才能进行下一个操作，这个简单的思想数十年来都是制造世界最快计算机的关键。自从 1980 年以来，坐落于加州劳伦斯利物默实验室[②]的克瑞巨型计算机，在保罗·盖奇（Paul Gage）和大卫·

---

① National Bureau of Standards，现在是美国国家标准与技术研究院 National Institute of Standards and Technology，NIST。

② Lawrence Livermore Laboratory 是美国的国家实验室之一。



斯洛文斯基（David Slowinski）的管理之下，经常打破纪录并登上新闻头条。到1996年，他们宣布发现了第十七个创纪录的素数，一个有378632位的素数 $2^{1257787}-1$。

不过近来，发现素数的潮流更偏爱年轻人。就像牧羊人大卫杀死巨人哥利亚一样，最新的纪录都是由个人计算机创造。究竟是什么给予他们挑战克瑞巨型机的能力呢？就是因特网。通过网络无数的个人计算机被整合到一起，这样组合起来的计算机网络具有挑战大素数的潜力。利用因特网使得业余爱好者也能进行科学研究，这并非首次，在天文学界，数千名业余天文学家每人都分配到一小片天空进行探索，然后通过因特网协调这些个人的行为。受到这件事的启发，一位美国程序员乔治·沃尔特曼（George Woltman）在因特网上公布了一个程序，下载这个程序的人都可以利用自己的计算机探索广袤数字世界中的一小部分。不同于天文爱好者利用望远镜搜寻夜空中的超新星，这些业余科学家们利用的是计算机的空闲时间，来搜索数字宇宙中的一角，期望可以发现新的素数。

207

然而，这样的搜索有时也会带来麻烦。沃尔特曼的一位成员受雇于美国一家电话公司，他想办法利用了公司内的2585台计算机帮他进行梅森素数的搜寻工作。电话公司发现菲尼克斯[①]的计算机经常会出些差错，本来只需要5秒钟就可以接通的电话号码，现在需要5分钟才能接通，于是公司开始怀疑是不是出了什么毛病。联邦调查局最终找到了问题的源头，这位雇员承认"被所有计算机的强大计算能力所引诱"，电话公司并没有为雇员追求科学的精神所感动，而是将他解雇。

这群因特网搜寻者的第一个发现，是一个新的梅森素数，这仅仅在1996年克瑞计算机宣布自己的结果之后几个月。一位巴黎程序员乔伊·

① Phoenix，美国亚利桑那州的首府和最大城市，位于该州的中南部地区，1868年建立，1889年成为地区性首府，1912年成为州首府。该城以疗养胜地而闻名，也称为凤凰城。



阿门高德（Joel Armengaud）在他加入沃尔特曼计划之后不久就挖到了金矿。对媒体而言，这样的发现距离上一个发现出现得太快。当我联系《时代》杂志询问有关最大素数的时候，他们告诉我几乎每一年他们都要报道这样的发现。而从1979年以来，克瑞研究所的斯洛文斯基和盖奇平均需要两年才能做出一个新的发现。

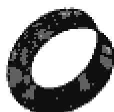
但是现在情况比发现新素数更好，这标志着计算机在搜索素数过程中所起作用的转折点。在专业的因特网杂志《连线》中，有一篇关于GIMPS计划的报道，GIMPS就是大因特网梅森素数搜寻计划（Great Internet Mersenne Prime Search），在报道中，沃尔特曼已经成功地吸引了全世界超过20万台计算机，组成了现今最为强大的并行处理计算机。这并不是说克瑞计算机已经失业，它也是计划的一部分，用来检验这些年轻人的发现。

208

到2002年，在搜寻梅森素数计划中已经出现了5位幸运者。排在巴黎人后面的是一位英国人，然后是一位加州居民。来自密歇根州普利茅斯的纳扬·哈贾瓦拉（Nayan Hajratwala）在1999年6月真正挖到了金矿，他发现的素数 $2^{6972593}-1$ 是一个2098960位的数，这也是第一个超过100万位里程碑的素数。除了这个数本身的意义之外，发现者同时获得了由电子前线基金会（Electronic Frontier Foundation）颁发的5万美元奖金。这个加利福尼亚的团体自封为网民——使用因特网的人——自由权利的捍卫者。如果你被哈贾瓦拉的成功所激励，这个基金会还有五十万美元等着发给那些找到更大素数的人，下一个里程碑被设在1000万位。哈贾瓦拉的纪录在2001年11月被加拿大学生麦克尔·卡梅隆（Michael Cameron）打破，卡梅隆用个人计算机证明了 $2^{13466917}-1$ 为素数，这是一个超过400万位的数。数学家相信，这样的梅森素数有无穷多，正等待着被发现①。

---

① 目前已知最大的素数是2006年9月4日由中密苏里州立大学的Curtis Cooper和Steven Bonne率领的团队发现的第44个梅森素数232 582 657 - 1，这个素数有9808358位。



计算机——数学的谋杀者？

如果计算机可以超越我们，那是不是意味着数学家就是多余的？事实并非如此，计算机并非数学末日的宣告者；相反，它更加突出了数学家作为创造性艺术家和计算机作为繁杂计算机器之间的差别。显然，计算机是数学家探索数学世界的强有力的新伙伴，是我们攀登黎曼峰的夏巴族同伴①。但是它永远不可能取代数学家，虽然计算机可以在任何有限的计算中轻松超越数学家，但是它缺少（就目前而言）用来描述无穷图像并解释数学中潜在结构和规律的想象力。

比如说，计算机对于大素数的搜索是否能让我们更好地理解素数？我们可以唱出更高的音符，但这并不代表着音乐。欧几里得已经告诉我们总有更大的素数等待我们去发现，但我们并不知道，用梅森的方法是否能找到无穷多个素数。也许麦克尔·卡梅隆发现的第39个梅森素数就是最后一个。当我和保罗·厄多斯交谈时，他认为证明存在无穷多个梅森素数这一命题是目前数论中未解决的难题之一。通常大家都认为可以选择无穷多个 n 使得 2^n-1 为素数，但是计算机是否能证明这一点，可能性不大。

209

但这并非说计算机不能证明任何命题。给定一系列公理以及推理规则，你就可以通过程序让计算机输出数学定理。关键在于，像猴子随意敲打打字机一样，计算机无法从小学的求和公式中分辨出高斯定理；而数学家已经发展出一种才能，可以分辨哪个定理重要，哪个定理不重要。数学思想的美学感受促使我们欣赏优美的证明，抛弃那些丑陋的证明。虽然丑陋的证明也是有效的，但是在我们确定数学世界中的最佳路

---

① 夏巴族，居住在喜马拉雅山脉南侧，尼泊尔和锡金境内的西藏人后裔，以他们的登山能力而闻名。1953年与新西兰人埃德蒙·希拉里一起登顶珠峰的尼泊尔向导丹增诺吉就是夏巴族人。

线时，证明的优美往往被认为是重要的判断标准。

利用计算机成功证明的第一个定理，与一个叫做四色问题的挑战有关。这个问题起源于一位数学爱好者的好奇心，同时也许是我们在儿时就已注意到的结果：如果要给一幅地图填上颜色，但是任意两个相邻的国家颜色不能相同，那么利用四种颜色就已经足够。除非国家的边界出现极端的情况，你会发现填满欧洲地图不需要更多的颜色。并且由法国、德国、比利时和卢森堡的国界线，可知我们至少需要 4 种颜色，但是怎么能证明对于任意的地图，4 种颜色就足够了呢？



图 33　至少需要 4 种颜色来给地图着色，才能使得任意两个相邻的国家颜色不同

这个问题最早出现于 1852 年。当时一位法律学生弗朗西斯·古特里（Francis Guthrie）写信给自己的兄长，伦敦大学的数学家，询问是否有人证明了四种颜色就足够。在当时，没有太多人认为这是一个重要的问题，一些数学家曾试图为古特里提供证明。但是，这样的证明一直也没有出现，人们意识到解决这个问题也许需要更多的数学才能。希尔伯特在哥廷根的最好朋友，赫曼·闵可夫斯基也在这个问题上碰壁。在闵可夫斯基的某次讲座上，有人提出了这个四色问题，“这个问题一直都是由三流的数学家在做，因此还没有得到解决，”闵可夫斯基宣称，“我相信我可以证明它。”他用了数次讲座的时间在黑板上进行演算。某天当他进入教室的时候，天空中突然想起一声惊雷，“看来上天也震怒

210



于我的骄傲，”闵可夫斯基说，“我的证明是不成功的。”

越来越多的人尝试征服这个问题，都以失败告终。由于它的表述特别简单，因此这个问题变得越来越有名。到了1976年，在古特里发出那封信之后100多年，它终于得到了解决。来自伊利诺斯大学的两位数学家肯尼斯·阿佩尔（Kenneth Appel）和沃尔夫冈·哈肯（Wolfgang Haken）证明了，并不需要对无穷多种可能的地图进行填色的分析，他们将这个问题归化为1500种不同的基本地图。这是重大的突破，就像是制图学中的元素周期表，利用这些基本地图，就可以生成所有的地图。但如果手工检验这些基本地图，即使他们两人从1976年就开始检查，一直到今天他们也许还在工作。因此，计算机首次被用来完成整个证明，在花费了1200小时的计算机时间后，计算机最终输出了最后的结果：是的，每幅地图都可以用4种颜色填完。人类的创造力证明了只需要考虑1500种基本地图，就可以证明所有的地图，再加上计算机强有力的计算能力，最终证实了古特里在1852年提出的猜想：对任何地图填色都只需要4种颜色。

然而，知道四色定理的正确性并没有任何实际的用途。制图者不会因为听到这个结果，知道不再需要买第五种颜色而长吁一口气。数学家也并非急切地需要知道这个结果才能进行后续的探索，他们没有看到有什么重要的结果依赖于这个定理。黎曼假设则不一样，有数千个结果依赖于它的证明。四色定理的重要性在于，它使我们明白了在二维空间都存在这样简单、但我们无法回答的命题。在没有得到解决的那么长时间中，它促使数学家对身处的空间进行更深的理解，这也是为什么有些人并不满意阿佩尔和哈肯的证明的原因，计算机给了我们答案，但却没能加深我们的认识。

211

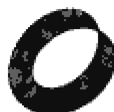
阿佩尔和哈肯借助计算机得到的四色定理的证明，是否真正符合“证明”的含义，仍然是大家争论的焦点。即使大家知道这样的证明比其他个人的证明都更有可能正确，但许多人还是因为计算机的介入而感

到不安，这样的证明能够促进理解吗？哈代曾经说过，“数学证明应该像星座那样有着简单清晰的轮廓，而不是散乱无章的银河。”四色问题的计算机证明只是对整个天空中所有的混乱进行了辛勤的检查，但并没有告诉我们更深的关于为什么天空是这样的理解。

这个在计算机帮助下得到的证明也说明了数学的乐趣并非仅仅来自于结果。我们阅读数学趣闻的时候不仅仅关心是谁解决了它，数学的喜悦来自于将众多混杂在一起的线索层层拨开，最终得到真相的那一瞬间。阿佩尔和哈肯关于四色定理的证明，让我们在阅读数学故事的时候失去了感受“啊哈！我知道了！”的喜悦，我们希望能够分享证明发现者当时体验到的精彩瞬间。关于计算机是否能够拥有情感的争论还将持续很久，但是四色问题的证明却不能让我们分享计算机可能感受到的喜悦。

抛开美学的感受，计算机仍将继续为数学界证明定理。如果一个问题可以归化为有限个条件的检验工作，那么计算机就可以发挥作用。那么计算机是否可以帮助我们在征服黎曼假设的道路上更进一步呢？在第二次世界大战末期、哈代去世的时候，大家普遍认为黎曼假设可能是错的。就像图灵所想的那样，如果黎曼假设是错的，那么计算机肯定能发挥作用，计算机可以用来检验零点，直到找到一个落在临界线之外的零点。但是如果黎曼假设是正确的，计算机将变得毫无作用，因为它无法证明这无穷多个零点都落在临界线上。计算机所能做的就是给出越来越多的证据，支持我们对黎曼假设的信心。

计算机也满足了另外的需求。到哈代去世时，数学家在黎曼假设这个问题上已经束手无策，与黎曼假设相关的理论已经走到尽头。看起来在现有的技巧之上，哈代、利特伍德和塞尔伯格对于可能计算的落在海平面上的点的位置，已经得到了最佳的结果，他们已经将这些技巧发挥到了极致。大部分数学家认为，如果要在证明黎曼假设的道路上继续前进，必须有全新的思想。由于缺少新思想，计算机在前进的过程中留下了印记，但仅仅是印记而已——计算机的加入掩盖了明显的关于黎曼假



设的新思想的缺乏，计算成为思想的替代物，是思想的暂时休憩，也是当我们面对障碍的时候，获得一段时间，可以用来好好的思考我们应该做些什么。

查吉尔，数学火枪手

西格尔于1932年从黎曼未发表手稿中发现的秘密公式，可以用来准确并且有效地计算黎曼世界中零点的位置。图灵曾试图利用自己的齿轮系统来加速这一计算过程，但是只有更加现代的机器才能认识到这个公式的真正潜力。一旦这个公式变成计算机程序，我们就可以探索黎曼世界中从未想象过的新世界。在20世纪60年代，当人类开始利用无人宇宙飞船探测遥远宇宙的时候，数学家也开始利用计算机来计算黎曼世界中到达遥远目的地的路程。

在搜寻零点的路途上，数学家越往北走，就能搜集到越多的证据。但是这些证据有什么用呢？究竟需要多少零点落在临界线上，才能让数学家觉得足够自信宣称黎曼假设是正确的呢？问题在于，利特伍德已经证明了，在数学中自信并非来自于证据。这也是为什么有些人觉得计算机并非探索黎曼假设有力工具的原因。然而，即将发生的一件事将令那些最顽固的怀疑论者相信，黎曼假设很有可能是正确的。

在20世纪70年代初，有一位数学家是这些怀疑论者的先锋。唐·查吉尔（Don Zagier）在现今的数学界中是一位充满活力的数学家，当他穿过德国马克思·普朗克数学研究所（这是德国对应于美国普林斯顿高等研究院的单位）的走廊时，总是那样地风风火火。和其他数学火枪手一样，查吉尔不断充实自己剃刀般锋利的思想，随时准备解决碰到的问题。他对于数学的热情和能量，表现在他急促并且快速的话语中，他表达出来的思想旋风，经常使听众屏息静气。他总是轻松地处理数学问题，并且总是在午饭的时候提出一些数学趣题作为佐餐的调料。



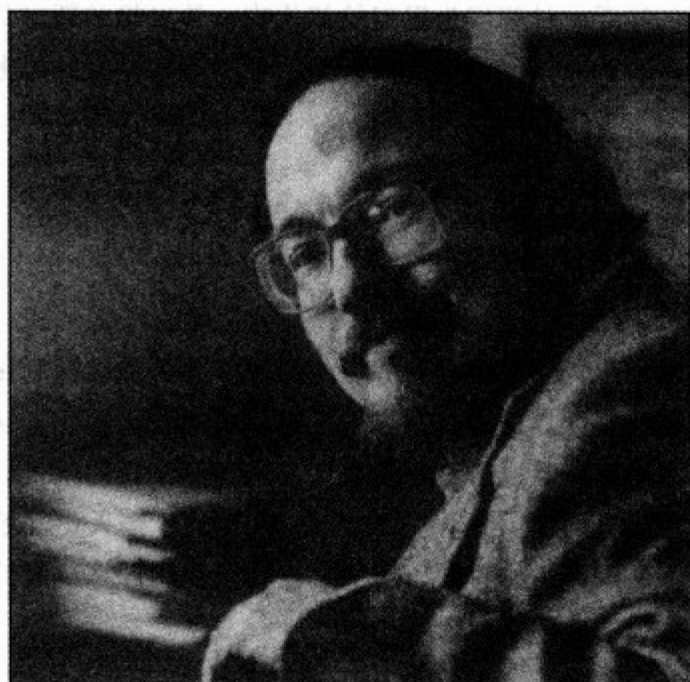


图 34 唐·查吉尔，马克思·普朗克数学研究所教授，波恩

查吉尔对于有些人仅仅从纯粹美学观念出发，无视其他的支撑证据就相信黎曼假设是正确的感到很愤怒。对于黎曼假设的信心等价于对数学中的简单性和优美性的尊敬，如果一个零点落在临界线之外，就像是优美图画中的一个污点。每个零点都为素数音乐贡献一个音符，如果黎曼假设最终被证明是错误的，邦比艾里这样描述它的意义，“就像是你去听一场音乐会，所有的音乐家都以和谐的方式演奏乐曲，突然大号发出一个很强的声音，掩盖了其他乐器的声响。”数学世界中存在着如此多的美，我们不能——也不敢——相信大自然会选择一个不和谐的宇宙，在其中黎曼假设是错误的。

但是，在黎曼假设这个问题上，查吉尔就是怀疑者的代表人物，而邦比艾里则是典型的信徒代表。在 20 世纪 70 年代，邦比艾里还没有去普林斯顿的时候，他是意大利的一名数学教授。查吉尔解释说，“邦比



艾里持有一种绝对的信心，相信黎曼假设是正确的。这像是一种宗教的信仰，如果它不正确，那么整个世界都将崩溃，因此它必须正确。”实际上，邦比艾里详细描述过这一点，“当我在十一年级的时候，我读过一些中世纪哲学家的东西，其中一位叫奥卡姆（William of Occam）。他提出过一个思想，当我们必须在两种解释中选择一个的时候，总是应该选简单的那一个。这就是奥卡姆剃刀的原则，排除困难的，选取简单的。”对邦比艾里而言，落在临界线之外的零点就像是管弦乐队中某件乐器“掩盖了其他乐器的声响——这是一种非美学的情形。作为奥卡姆剃刀的忠实信徒，我拒绝接受这个结论，因此我相信黎曼假设是正确的。”

当邦比艾里访问波恩马普数学研究所的时候，故事发展到了高潮。茶点时间的讨论不可避免地谈到了黎曼假设。查吉尔这位霸道的数学家，终于有机会对邦比艾里进行一次双重挑战，“我在茶点时间告诉他目前还没有足够的证据来令我相信黎曼假设是正确的，因此我愿意和他对此事立下等额赌约。但这并不表明我认为黎曼假设错误，而是我愿意充当魔鬼的代言人。”

邦比艾里答应了他，“好，我愿意接受你的挑战。”查吉尔意识到自己犯了一个错误，他不应该提出等额赌约——因为邦比艾里是如此地坚信黎曼假设正确，他应该提出一个像10亿比1这样的赌约。同时双方约定了赌约的内容：赢家任选两瓶上好波尔多葡萄酒。

“由于我们希望这样的赌约应该在我们有生之年结束”，查吉尔说，“然而在我们走进坟墓之时，黎曼假设得不到解决的可能性相当大。同时我们也不希望加上一个时间限制，比如说如果10年没有解决，那么这个赌约就废除。这看上去太没有意思，10年时间对于黎曼假设根本算不了什么，因此我们希望某些数学上的结果。”

于是查吉尔提出了新的赌约内容。虽然图灵的机器在计算了前1104个零点坐标之后就崩溃了，但是到1956年，德里克·莱默已经获得了



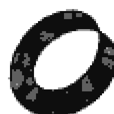
一定的成功。他利用加利福尼亚的机器检查了大约前25000个零点，它们都落在临界线上。到了20世纪70年代初，一次有名的计算已经确认前350万个零点都落在临界线上。其中的证明非常出色地利用了一些绝妙的理论技巧，将计算推进到了当时的计算机技术所不能达到的那个极限。对此查吉尔说道，

215

> 因此我说，好，现在已经计算了300万个零点，即使大部分人都会说"你究竟想要怎样……我的天……300万个零点"，但是我仍然不相信。大部分人又会说"还有什么可以改变的呢，300万和30000亿有什么差别"，这正是我们要告诉你的关键点。话不是这样说的，300万的零点并不能说服我，我希望这个赌约应该是更早立下，那样我现在就已经开始相信了。我也希望自己定的赌约是前10万个零点，在那样的时候根本没有理由相信黎曼假设。因为在你分析数据的时候，10万个零点根本毫无用处，它本质上没有提供任何证据。300万个零点才使得问题有点意思。

但是查吉尔知道3亿个零点代表着重要的分水岭。理论上的分析告诉我们最初的数千个零点肯定是落在黎曼的临界线上，但是当你走得越远，保证零点落在临界线上的理由就开始被更强的理由超过，而这个理由说明零点应该落在临界线之外。查吉尔知道，如果到了前3亿个零点时，这些零点仍然落在临界线上，那么一定有某个更加奇妙的东西在起作用。

基于自己的分析，查吉尔用一幅图像来表示黎曼临界线上高峰和低谷的倾斜度。查吉尔的图像通过观察穿越临界线的截面，给出了研究黎曼世界的一个新角度。有意思的是这也为黎曼假设带来一种全新的解释。如果这个新的图形和黎曼临界线相交，那么肯定会有一个零点落在临界线之外，那么黎曼假设就是错误的。刚开始的时候，这个图形应该与临界线保持一定距离，实际上是一条上升的曲线，随着你越往北，这个图形开始下降，渐渐逼近临界线。查吉尔的每一个图形都试图撞击临



界线，但是正如下图所示的那样，总有一些东西在阻止这条曲线与临界线相交。

因此，只要你向北方前进得足够远，看上去这个图形就可能与临界线相交。查吉尔知道第一个有希望的地方差不多是在3亿个零点左右，因此临界线的这一区域应该被认真地检查。如果向北方已经走到了这么远，仍然不能发生相交的现象，那么肯定有某种原因阻止它们相交。而这个原因，查吉尔猜测应该就是黎曼假设之所以正确的原因，这也就是查吉尔为什么将赌约定在3亿零点的原因。如果黎曼假设被证明正确，或者在前3亿个零点位置的计算中找不到反例，那么邦比艾里将赢得这场赌局。 216

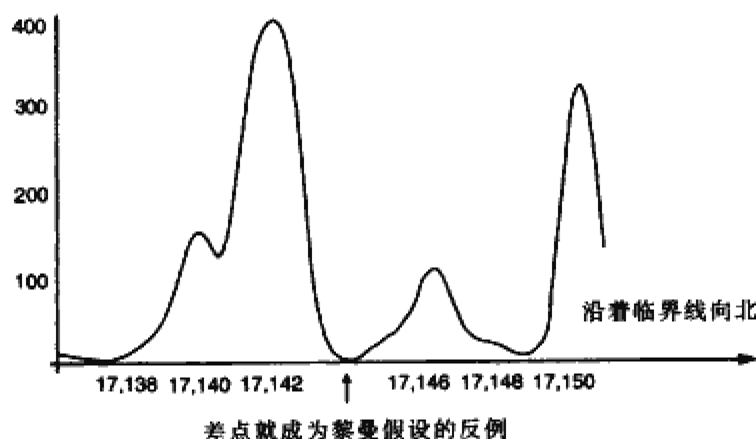


图35　查吉尔的辅助图形——如果这个图形与水平轴相交，那么黎曼假设是错误的

查吉尔知道70年代计算机的能力还很弱，无法探索黎曼临界线的这一区域。他估计，计算机已经设法计算出了前350万个零点的位置，考虑到计算机科学随着时间的发展，大概需要30年的时间，才能计算到第3亿个零点。但是他却没有考虑到正在发生中的计算机革命。

随后的5年没有任何新发现。尽管计算机的能力在缓慢地增长着，但计算700万个零点需要花费的时间也是原先的一百倍，因此没有人去



考虑这些计算。毕竟，在这件事上没有人愿意花费这样长的时间，仅仅是将证据数增加为两倍。但是，5 年之后，计算机的速度突然得到了大幅提高，因此两个小组接受挑战，利用计算机全新的能力来计算更多的零点。其中一个小组位于阿姆斯特丹，领导者是赫曼·特瑞利（Herman te Riele）；另外一个位于澳大利亚，领导者是理查德·布兰特（Richard Brent）。

布兰特首先于 1978 年宣布，7500 万个零点都落在临界线上。随后阿姆斯特丹的小组加入了布兰特的小组，一年之后，他们合作写出了一篇长文，语句精练，措辞优美，每一点都恰到好处。他们的结果是……

217

2 亿个零点！查吉尔笑了，

> 我长长地出了一口气，这是一项了不起的计划，也要感谢上帝让他们幸运地停在了 2 亿处。显然他们可以做到 3 亿，但是他们没有。这样我又可以轻松几年了，他们不会为了百分之五十的提高而再次尝试。我们下一次等来的应该是 10 亿的结果，显然这又需要不少时间。不幸的是，我没有考虑到我的好朋友亨德里克·兰斯特拉（Hendrik Lenstra），他知道我的赌局，并且他当时也在阿姆斯特丹。

兰斯特拉问特瑞利，“为什么你的小组只计算到 2 亿的零点？要知道，如果你们计算了前 3 亿个零点，唐·查吉尔将输掉一个赌局。”因此这个小组继续把工作推进到了 3 亿，显然他们并没有发现一个落在临界线之外的零点，因此查吉尔必须付清赌金。查吉尔带着两瓶酒找到了邦比艾里，邦比艾里和他分享了一瓶。后来查吉尔指出 ，这也许是他喝过的最昂贵的酒，因为，

> 2 亿个零点对我的赌局没有任何影响，他们是独立完成的工作。但是他们进行后 1 亿个零点的计算，却是因为听说了我的赌局。为了计算后 1 亿个零点，他们大概花费了 1000 小时的 CPU 时间，而当时 1 小时 CPU 时间的代价是 700 美元。由于他们进行这个计算只是



> 为了看到我输掉赌局，买上两瓶好酒，因此我可以说一瓶酒的价值是35万美元——这比任何拍卖会上卖出的酒都要昂贵。

但更重要的是，在查吉尔看来现在的证据已经足够支持黎曼假设的正确性了。作为计算工具的计算机终于强大到可以在黎曼的ζ函数世界中探索得足够远，对那些可能产生反例的区域进行探索。查吉尔的辅助图形对黎曼临界线作出无数次的冲击，但是显然有某种东西像反作用力一样阻止这个图形与临界线相交。原因是什么呢？那就是黎曼假设。

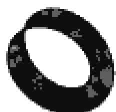
现在查吉尔承认，"这件事使我成为黎曼假设的忠实信徒。"他将计算机在这方面的应用比喻为粒子加速器在理论物理学上的应用。物理学家对物质的构成有一个模型，但是如何测试这个模型，就需要生成巨大的能量来轰击原子。对查吉尔而言，3亿个零点已经产生足够大的能量，来检验黎曼假设是否可能正确：

> 这个，我相信，是百分之百的证据让我确信肯定有某种东西阻止图形和临界线相交，而我能想象到的唯一可能发生的事就是，黎曼假设确实正确。现在我和邦比艾里一样，绝对是一个坚信黎曼假设正确的人，并非因为它是如此美妙，如此完美，或者是因为上帝的存在，而是因为有了充足的证据。

218

特瑞利在阿姆斯特丹的小组成员之一让・范德鲁恩（Jan van de Lune）现在已经退休。但是数学家从来也不会完全放弃对数学的痴迷，即使他们已经离开了工作岗位。利用自己小组在数10年前使用的程序，以及家中的三台个人计算机，范德鲁恩确认了前63亿个零点都符合黎曼假设。但是无论计算机能计算多少个零点，它也无法以这种方式生成一个证明。但是如果有一个零点落在临界线之外，那么计算机就在探索黎曼假设的进程中起到了非常重要的作用。

这也正是计算机擅长的工作——猜想的终结者。在20世纪80年代，关于零点的计算摧毁了黎曼假设的兄弟——梅腾斯猜想（Mertens



Conjecture)，但是这一计算结果并非来自意料中的数学系，而是来自一个意料之外的地方：AT&T 电话公司。

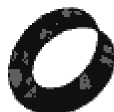
奥德兹克，新泽西的计算大师

在新泽西的核心地带，靠近宁静小镇佛洛汉庄园（Florham Park），一个看上去不可能产生新的数学能量的地方，却在 AT&T 研究实验室的商业资助之下迅速崛起。如果你有幸进入过这些建筑物，你会误以为身处某个大学的数学系之中，但这里确实是电信商业的发源地。实验室的起源可以追溯到 20 世纪 20 年代，当时 AT&T 贝尔实验室刚刚成立，图灵也曾在纽约的贝尔实验室待过一段时间。图灵参加的项目是设计一种语音加密系统，这样华盛顿和伦敦之间就可以进行安全通话。图灵曾说，自己在贝尔实验室的日子过得比在普林斯顿有意思得多，当然这与曼哈顿热闹的夜生活多少也有点关系。厄多斯在自己的数学交流中也经常访问新泽西。

在 20 世纪 60 年代，科技的蓬勃发展深深地影响了电信工业。AT&T 知道，要想保持行业的领先地位，必须掌握越来越复杂的数学知识。由于 60 年代高校的迅速扩张，伴随 70 年代而来的是许多数学毕业生的失业。为了扩充自己的研究机构，AT&T 吸引了这样的一些人才。虽然 AT&T 希望这些研究工作最终可以转化为科技创新，但是他们同样鼓励数学家继续追求自己的数学事业。看上去好像很无私，实际上这是很精明的商业：由于 AT&T 在70年代的垄断地位，它在如何分配利润方面受到了许多限制，而投资研究实验室则是吸收部分利润的恰当途经。

219

不论 AT&T 的动机是什么，对数学而言总是有利的。许多很有趣的理论进展都来自于该实验室的想法，这是学术与精明商业世界的完美组合。在一次访问该实验室并作报告的过程中，我亲眼目睹了这种融合。AT&T 希望在移动电话带宽的拍卖中获得最大限度的标的，面对这个问题，一些数学家在午餐时提出了一个理论模型，能够为公司在复杂的竞



标过程中提供最佳策略。对数学家而言，这就像是象棋游戏中的策略，而非如何使用数百万美元的策略，但是两者并无差别。

在2001年之前，这个实验室的领导人是安德鲁·奥德兹克（Andrew Odlyzko）。奥德兹克来自波兰，至今仍然保持着明显的东欧口音。他在商业部门的经历让他成为一个很好的讲解者，即使是面对很复杂的数学思想。他的话语中有一种包容的态度以及不可抗拒的力量，鼓励你加入他的数学征途。但是奥德兹克是一个细致的、完美主义的数学家：每一步都不能存在含糊不清的地方。当奥德兹克在麻省理工学院的哈罗德·斯塔克（Harold Stark）的指导下攻读博士学位时，他开始对ζ函数产生了兴趣，因为有一个问题需要知道ζ函数世界中最初那些零点的准确位置。

在高精度计算方面，计算机远远胜过人类。在奥德兹克加盟AT&T贝尔实验室后不久，他就取得了突破。1978年，实验室购买了第一台超级计算机——克瑞一号，这是克瑞计算机首次被政府或高校之外的私人公司拥有。由于AT&T是一个商业机构，财政预算和开支支配着所有一切，因此这台计算机是所有部门共用的。然而，职员需要一定的时间来学习如何编写可以运行在克瑞计算机上的程序，因此在刚开始的时候，这台计算机并没有得到太多的应用。所以计算机部门决定为那些没有得到资助的科学计划提供5小时的免费使用时间。

220

这个探索克瑞计算机能量的机会对奥德兹克而言是无法抗拒的。于是奥德兹克联系阿姆斯特丹和澳大利亚的小组，询问他们既然已经证明了前3亿个零点都落在临界线上，那么他们有没有精确地计算这些零点在临界线上的位置，两个小组的回答都是否定。他们的重点都放在证明黎曼当初预测的，这些零点的东西坐标为1/2，而没有关注这些零点的南北坐标。

于是奥德兹克申请使用克瑞计算机的免费时间，用来计算前100万个零点的准确坐标，AT&T同意了。此后的数十年，奥德兹克一直利用公司计算机的空闲时间，计算越来越多的零点坐标。这样的计算并非是

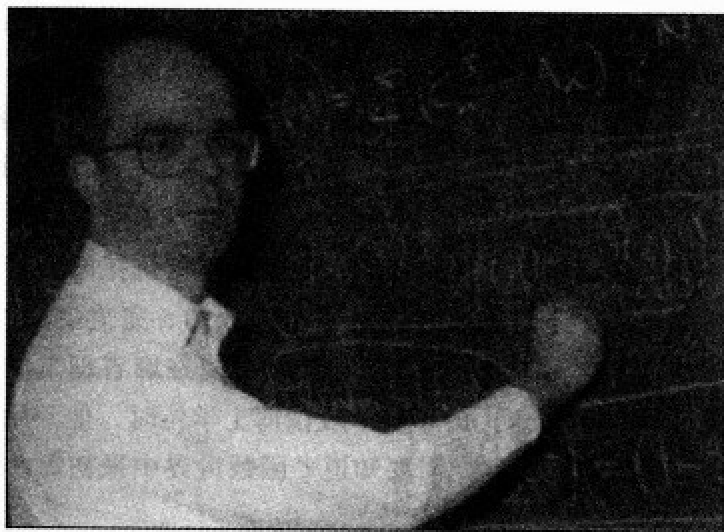


图 36　安德鲁·奥德兹克，AT&T 研究实验室领导人，2001 年卸任

没有动机的行为，奥德兹克的导师斯塔克曾经利用从最初几个零点位置获得的信息，证明了高斯的一个猜测——某些虚数集合可以被分解。同样，奥德兹克利用最初 2000 个零点的准确位置，推翻了一个从 20 世纪开始就困扰数学界的猜测：梅腾斯猜想。他参加了特瑞利在阿姆斯特丹的小组，希望推翻这个猜想，特瑞利就是验证了前 3 亿个零点都落在黎曼临界线上，从而让查吉尔输了赌局的那位数学家。梅腾斯猜想与黎曼假设有很大的关系，它被推翻的事实让数学家明白，如果黎曼假设是正确的，那么它就是恰好正确。

221

我们同样可以利用扔素数硬币这个游戏来理解梅腾斯猜想。在第 N 次扔出梅腾斯硬币时，如果 N 由偶数个素数构成，那么这枚硬币正面朝上。比如说 $N=15$，那么 15 是由两个素数 3 和 5 构成，因此结果是“正面”。另一方面，如果 N 是由奇数个素数构成，比如 $N=105=3\times5\times7$，那么结果就是“反面”。然而还有第三种情况，如果 N 的某个素因子出现了两次，那么结果就记作零：比如说 12 由两个 2 和一个 3 构成（$12=2\times2\times3$），那么结果就是零。我们可以将零这个结果认为是硬币扔丢



了或是立在地面上。因此梅腾斯是对 N 越来越大时硬币的行为做出的猜想，这个猜想非常类似于黎曼假设，黎曼假设认为素数硬币是没有偏差的。但是梅腾斯猜想比黎曼假设对素数的预测要稍微强一些，它预测硬币误差将比一个公平硬币的误差稍小。因此如果这个猜想正确，那么黎曼假设就是正确的——但是反之不然。

在 1897 年，梅腾斯制作了一张表，其中包括了直到 $N=10000$ 的素数来支持自己的猜想。到了 20 世纪 70 年代，实验证据已经达到了 10 亿。但是，正如利特伍德所说，数十亿的实验证据也不能说明任何问题。在很多人开始觉得梅腾斯猜想是正确的时候，奥德兹克和特瑞利将前 2000 个零点的位置计算到了 100 位的精度，终于否定了梅腾斯猜想。同时，奥德兹克和特瑞利给出的另一个结果还警告了那些被大量数值证据征服的人，即使梅腾斯对 10^{30} 以内的数都进行验算，所有的结果都完全符合他的猜想（这意味着在 10^{30} 之内不会出现反例），但梅腾斯猜想仍是错的。

奥德兹克利用 AT&T 的计算机继续帮助数学家探索素数的奥秘。但是这并不是一个单向的应用，现在素数也开始对快速发展的计算机时代作出自己的贡献。在 20 世纪 70 年代，素数成为电子通信中隐私保护的关键。哈代曾经非常骄傲地认为，数学特别是数论在真实世界中没有应用： 222

> “真正”的数学家所研究的“真正”的数学，如费马、欧拉、高斯、阿贝尔和黎曼研究的数学，几乎是完全“无用”的。（这一点对“应用”数学和“纯”数学来说都是如此。）以“实用性”为标尺来衡量一个天才数学家的工作是不可能的。

哈代在这一点是完全没有预想到，费马、高斯和黎曼所研究的数学将被应用到商业世界的核心中，这也是为什么 AT&T 在 80 年代和 90 年代招募更多数学家的原因。电子世界的防卫措施是否能够坚持或是崩溃，完全依赖于我们对于素数的理解。 223

第十章

破解数字和密码

如果高斯活在当代，他肯定会是一名黑客。
——彼得·萨那克（Peter Sarnak），普林斯顿大学教授

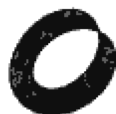
在 1903 年，纽约哥伦比亚大学的数学教授弗兰克·内尔森·科尔（Frank Nelson Cole）为美国数学会做了一场有趣的演讲。他一言不发，在黑板一边写下一个梅森数，在另一边写下两个数的乘积，在中间划上一个等号，然后坐下结束了演讲。

$$2^{67}-1=193\ 707\ 721\times761\ 838\ 257\ 287$$

所有的听众都站起来鼓掌，这在数学界中是很难得见到的景象。即使对于 20 世纪初的数学家而言，将两个数相乘并不是很难的事，但他们为何如此激动？因为科尔所做的工作正好相反。在 1876 年数学家已经知道这个 20 位的梅森数 $2^{67}-1$ 不是素数，而是两个更小的数的乘积，然而没有人知道这两个数是什么。利用三年中的每个星期天下午，科尔终于分解出这个数的两个素因子。

并非只有科尔 1903 年的听众欣赏这一点。在 2000 年，一场小范围的非百老汇剧《五姑娘定理》利用一位姑娘再现当年的计算向科尔致敬。在这场表现一个数学家庭去海边度假旅游的戏剧中，素数反复出现，其中的父亲为女儿即将年满 18 岁而感到伤心，并不是因为她到了 18 岁就会与她的情人私奔，而是因为 17 是一个素数，而 18 竟然可以被 4 个数整除！

2000 多年之前，古希腊人就证明了每个数都可以写成素数的乘积。



但一直以来，数学家都没有找到一个快速并且有效的方法找出某个数的素因子。对于化学家而言，光谱学可以告诉他们究竟是元素周期表中的哪种元素构成了某种化合物，数学界正是缺少类似的理论。如果能在数学中发现类似的结果，将所有的数都分解为基本的素数，那么发现者获得的荣誉绝对是超越学术界的。

科尔在 1903 年进行的计算被认为是数学趣闻——他获得的掌声主要是献给他艰苦的工作，而非问题本身蕴涵的重要性。现在，这样的素数分解问题已不再是周日下午用来打发时间的游戏，而成为了现代密码破译的核心。数学家已经发明了一种方法，将这样的素数分解难题融入到了密码中去，从而保护因特网上的金融安全。银行和电子商务公司利用 100 位的整数来保证自己金融传输的安全，赌的就是——在目前——找到这些整数的素因子需要极长的时间。同时，这些新的数学密码也被用来解决密码学中的一些顽固问题。

224

网络密码的诞生

自从人类有了信息交流之后，就需要传输一些秘密的信息。为了防止重要信息落到那些不应得到它们的人手中，我们的祖先发明了一些聪明方法来隐藏信息的内容。大约 2500 年之前，斯巴达军队发明了一种加密方法。发送者和接收者都有一个同样直径的圆柱体，称为 scytale。在加密信息的时候，发送者将窄窄的一条羊皮纸螺旋状地绕在圆柱体上，然后将信息沿着圆柱体的母线方向写在羊皮纸上，当羊皮纸展开之后，上面的信息看上去就毫无意义。这张羊皮纸上的信息只有在绕到同样直径的 scytale 上时，才能再次出现。此后，一代代的人们发明了许多复杂的加密方法，终极的机械加密装置就是第二次世界大战中，德国军方使用的 Enigma 密码机。

在 1977 年之前，任何想要传送秘密信息的人都不可避免地碰到一个问题。在传送信息之前，发送者和接收者必须事先决定选用哪一种密



码系统。比如说，斯巴达军队的将军必须确定使用的 scytale 的直径，即使是大量生产的 Enigma 密码机，柏林总部也必须指派情报人员将如何设置机器密码的手册送给潜艇和坦克部队，以便每天使用不同的设定。当然，如果敌人获得了这本密码手册，战争也就结束了。

我们设想一下，如果将这样的密码系统应用在现在的网络商务上会发生什么。在我们安全发送每天的银行账目之前，我们必须从网络公司那里收到秘密信件，告诉我们加密信息的方法。由于因特网每天都交换着海量的信息，这样的秘密信件很有可能被别人截获。因此，我们需要一种适应快速全球通信时代的加密系统。在布莱切利庄园中数学家破解了战时的 Enigma 密码，现在同样是数学家发明了新一代的编码方式，将密码学从间谍小说中释放出来融入到地球村的通信中。正是这些数学编码保证了“公钥密码系统”的诞生。

225

我们可以将加密和解密的过程，看作是给一扇门加锁和解锁的过程。对通常的门而言，一把钥匙既可以锁门也可以开门。对 Enigma 加密机而言，用来加密信息的设置与解密信息的设置是一样的，这样的设置——称为密钥——必须严格保密。接收者离发送者越远，那么传送加密或解密的密钥就越难以保密。假设一位间谍首脑希望手下不同领域的间谍人员都向自己发送安全的汇报信息，但是又不希望他们读懂其他人的报告，因此对每个手下需要用不同的密钥。现在如果将这些间谍人员换成数以百万计的网络购物者，对于如此规模的业务，虽然不是不可能，但也是后台程序人员的噩梦。某位顾客访问网站时，他不能立即下订单，而需要等待网站传送过来的安全密钥。因此“世界万维网”（World Wide Web）就变成了“世界等待网”（World Wide Wait）。

公钥密码系统就像是一扇有两把钥匙的门：钥匙 A 用来锁门，而另外一把钥匙 B 用来开门。我们不需要对钥匙 A 进行加密，因为拥有钥匙 A 并不会对安全造成任何危害。现在，假设这扇门通往公司网站的秘密区域，对那些希望访问网站并传送安全数据（比如说信用卡号码）的用户，公司可以自由地将钥匙 A 分发给所有人。即使所有的人都使用同样



的钥匙来对数据进行加密——将秘密锁在门内——也没有人可以查看其他人的加密信息。实际上，这些数据一旦进行了加密，用户就无法查看，即使是自己的数据。只有网站的拥有者知道钥匙 B，只有他可以打开这扇门，并查看其中的信用卡号码。

公钥密码系统在 1976 年首次由加州斯坦福大学的两位数学家在一篇重要论文中提出。维特·迪菲（Whit Diffie）和马丁·黑尔曼（Martin Hellman）也因此带动了密码学世界的反正统文化，对政府机构在密码学中的垄断地位发起了挑战。尤其是迪菲，他在 20 世纪 60 年代就是反正统的长发青年。他们两人都认为密码学不应该是在政府机构围墙之中进行孤立研究的学科，因此自己的思想应该为了个体的利益向大众公开。后来我们知道，这样的密码系统早已被一些政府机构了解，但是并没有在学术杂志上发表，而是盖上"最高机密"的印章后封存起来。

226

斯坦福小组的文章标题叫做"密码学的新方向"，它标志着密码学和电子安全的新时代。具有两把不同钥匙的公钥密码系统在理论上很完美，但是能否将这个理论转化为实际应用，创造一套全新的照此原理工作的编码理论呢？经过数年的努力，一些密码学家开始怀疑，这样的密码系统并不能设计出来。他们担心这种学术上的锁并不能对付真实世界中的间谍。

RSA，MIT 三剑客

在众多受到迪菲和黑尔曼论文影响的人中，有一位是麻省理工学院的罗恩·瑞威斯特（Ron Rivest）。与迪菲和黑尔曼的反叛性格不同，瑞威斯特是一位循规蹈矩的人。他言语不多，说起话来轻声细语，应付周围的世界显得很有分寸。当他读到"密码学的新方向"的时候，他的志向是成为某个学术机构中的一员，他关心的是教授职位以及数学定理，而不是间谍和密码。他并不知道，读了这篇文章之后，自己将踏上一条创造人类历史上最强大、商用最成功的密码系统之路。



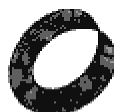
在斯坦福和巴黎进行研究工作之后，瑞威斯特于 1974 年加入麻省理工学院的计算机科学系。和图灵一样，瑞威斯特对于抽象理论和真实机器之间的交互非常感兴趣。在斯坦福的时候，他曾做过一些自动机器人，但是很快他的思想就转到了计算机理论科学方面。

在图灵的时代，计算的主要问题是围绕着希尔伯特第二和第十问题展开的，也就是讨论在理论上是否存在某个程序，可以解决某一类的问题。正如图灵告诉我们的，不存在这样的程序，可以用来判断数学真理是否存在证明。到了 20 世纪 70 年代，另一个不同的理论问题困扰着计算机科学的学术圈。假设存在一个程序可以解决某个特殊的数学问题，那么是否有可能分析这个程序需要多长时间来解决这个问题？如果这个程序需要付诸实施，这个问题就显得非常重要。解决这个问题需要大量的理论分析，同时它也是很实际的问题，这样的组合对瑞威斯特而言就是最好的挑战。于是他抛开斯坦福的机器人，来到麻省理工学院从事这门新开创的计算复杂性学科的研究。

227

"有一天，一位研究生交给我这篇论文说，'这个你也许会有兴趣'，"瑞威斯特回忆说。学生交给他的正是迪菲和黑尔曼的文章，很快瑞威斯特就被吸引住了。"这篇文章说明了什么是密码学以及它将是什么样的，你需要做的就是提出一个新思想。"这篇文章的挑战综合了瑞威斯特的所有兴趣：计算、逻辑和数学。这是一个明显具有实际应用的问题，同样它也与瑞威斯特心中盘旋不去的理论兴趣有着直接的联系。"在密码学中你要关心的就是如何区别简单问题和困难问题，"瑞威斯特说，"这也正是计算机科学关心的问题。"如果某个密码极难破解，那么它肯定是基于某个无法轻易算出结果的数学问题。

瑞威斯特开始试图建立一个公钥密码系统，于是他开始在自己已知的问题中寻找那些计算机需要耗费极长时间才能解决的问题，同时他也需要其他同事进行这方面的讨论。当时的麻省理工学院已经开始试图打破某种大学的传统，放松各系之间的界限，以促进学科之间的交流。瑞威斯特作为一位计算机科学家，他和一些数学系的同事在同一楼层共



事。附近的办公室里有两位数学家，他们是莱昂纳德·阿德曼（Leonard Adleman）和阿迪·沙米尔（Adi Shamir）。

阿德曼的性格比瑞威斯特外向，但仍然是一位典型的学术人士，他经常有一些超出实际的大胆和奇妙的想法。阿德曼回忆某天早晨走入瑞威斯特办公室的情形："罗恩坐在办公桌前，拿着一叠手稿，'你看过这些从斯坦福过来的关于密码的文章了吗？秘密代码、不规则性，嘿嘿嘿……'我的回答是，'是吗？很好，但是罗恩，我有一些更重要的事需要讨论，我不能分心。'但是罗恩对此非常感兴趣。"当时阿德曼关心的是高斯和欧拉的抽象世界，对他而言真正重要的是攻克费马大定理，而不是新潮的密码学。

在走廊远处沙米尔的办公室中，瑞威斯特找到了自己的听众——这位访问 MIT 的以色列数学家。他们两人一起，开始寻找某些可以用来实现迪菲和黑尔曼梦想的方法。虽然阿德曼对此并非很感兴趣，但瑞威斯特和沙米尔对这个问题的沉迷让他无法视而不见。"每次我路过他们办公室的时候，他们都在讨论这个问题。他们的大部分想法都失败了，由于我正好在那里，因此我随时可以加入讨论，判断他们提出的某个想法是否有道理。"

228

当他们在"困难的"数学问题中搜寻的时候，萌芽状态的密码系统也开始考虑更多数论中的问题。这正好是阿德曼的专长："既然这是我擅长的领域，有了我，他们的系统分析更加有效——大部分情况之下没有他们也行。"对阿德曼而言，瑞威斯特和沙米尔提出的看上去非常安全的系统是自己的最佳目标。经过一整夜在数论领域中的工作，他知道了如何破解这个最新的密码系统。"这样的情况一遍又一遍发生，我们外出参加滑雪旅行的时候，我们讨论的就是它……甚至在我们坐缆车到达滑雪道顶端的时候，我们讨论的还是它……"



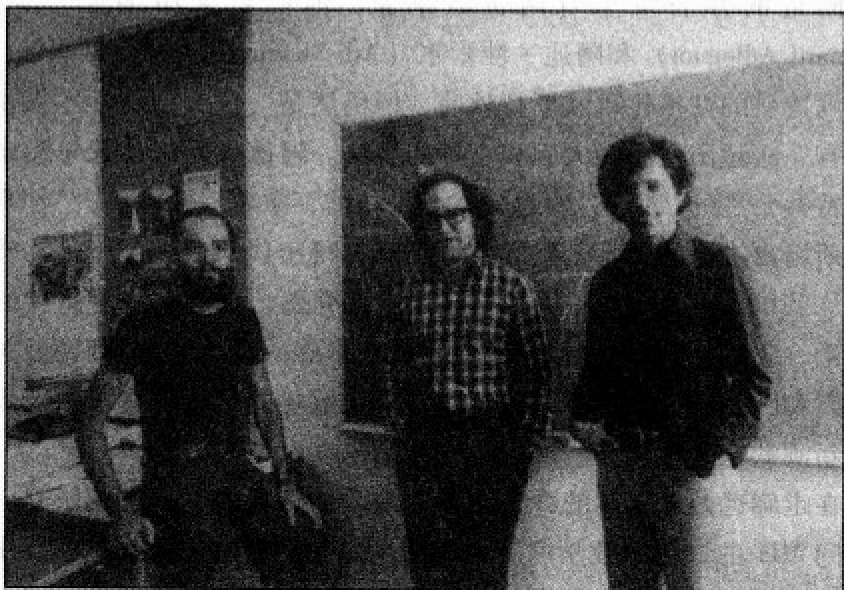


图 37　阿迪·沙米尔、罗恩·瑞威斯特和莱昂纳德·阿德曼

有一次，他们三人被邀请参加一位研究生家中举办的逾越节①宴会，当天晚上，事情终于有了突破。阿德曼没有喝酒，但是他记得瑞威斯特喝了不少宴会上的酒。在阿德曼于午夜回到家不久，瑞威斯特打来电话，“我有了一个新想法……”阿德曼仔细地听着，然后说“罗恩，我觉得这次可以了，这个想法不错。”他们把这个分解整数的问题又想了一会，发现目前还没有有效的程序，可以轻易地将一个整数分解为它的素因子，这正是他们需要的问题。带着酒意，瑞威斯特似乎已经明白如何将这个问题融入到编码中去。瑞威斯特回忆道，“一开始我的感觉很好，但是经验告诉我们开头的好感觉并不一定代表完美的结果，于是我决定将它留到第二天早晨再考虑。”

229

第二天上午，当阿德曼到达学校办公室的时候，瑞威斯特用一份手

① Passover，逾越节。开始于犹太教历 7 月 14 日，并按惯例持续 8 天的节日，用来纪念犹太人从埃及的奴役下解放出来。



写的草稿欢迎他，在草稿的最上方写着阿德曼、瑞威斯特和沙米尔的名字[①]。阿德曼简略地阅读了手稿，明白这正是昨天晚上瑞威斯特在电话中提到的想法。"于是我告诉罗恩'把我的名字去掉，这是你的工作'，然后我们就为了是否应该留下我的名字争论起来。"最后阿德曼同意再考虑考虑。当时阿德曼认为这篇文章也许会是自己文章中读者最少的一篇，因此留下名字也无所谓。但是他记得自己曾经为最初的密码系统进行整夜的工作，阻止了他们将一套不安全的密码付诸出版，让他们免于被指责。"于是我走回罗恩的办公室，'我做第三作者好了。'于是这就是 RSA[②] 的来历。"

瑞威斯特认为，他们应该了解分解整数这个问题究竟有多难。"在当时人们对分解整数问题的难度并不是很清楚，几乎没有什么文献谈到这个问题。对于运行那些已有算法所耗费的时间，也无法得到较好的估计。"恰好有一个人在这方面懂得比别人更多一些，他就是马丁·加德纳（Martin Gardner），一位世界知名的数学科普作家。加德纳对瑞威斯特的方案很感兴趣，并且应瑞威斯特的要求在《科学美国人》（*Scientific American*）的专栏上写了一篇关于这个思想的文章。

加德纳的文章引起了巨大的反响，阿德曼明白他们正在做一件了不起的事：

> 那年夏天我在伯克利的一家书店闲逛，一位顾客和老板正在讨论某件事情。那位顾客说，"你看了《科学美国人》上面关于密码的文章吗？"我走过去，"嘿，我就是其中一个作者。"那个年轻人看着我说，"那我能要你的签名吗？"在我一生中有几次被人要求签名？零！哇，这种感觉……真是意想不到！

230

---

① 国外对于合作的论文，一般按照作者姓名的首字母排序，因此阿德曼排在第一位，瑞威斯特第二，沙米尔第三，但在下文我们可以看到，事实并非如此。

② RSA，即为三个人的姓的首字母。



加德纳在文章中还提到，只要读者寄给三位数学家一个贴好邮资的信封，就可以免费得到文章的预印本。“当我回到 MIT 的时候，收到了数千封来自全世界的信件，毫不夸张，就是数千封，包括保加利亚国家安全局，呵呵呵！”

人们告诉这三位数学家，他们将会很有钱。在 20 世纪 70 年代，电子商务几乎无法想象，但是人们知道这个思想的潜力。阿德曼认为在几个月内美元就会源源不断地流进自己的口袋，于是毫不犹豫地给自己买了一台红色跑车。因此邦比艾里并不是因为数学上的成功而得到跑车的唯一一人。

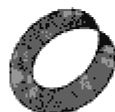
最终阿德曼用自己在 MIT 的工资偿还了跑车的分期付款。经过一段时间之后，情报和商业机构终于明白了 RSA 密码系统的强大。当阿德曼一边驾驶自己的跑车一边思考费马问题的时候，瑞威斯特开始考虑如何将这个设想付诸于真实世界中的应用：

> 我们认为这个方案也许会有某些商业应用，于是在 MIT 将它申请了专利，看看是否有某些公司对此有兴趣，并将其产品化。但是在 20 世纪 80 年代初期，确实没有任何市场。在当时，几乎没有公司对它感兴趣，因为整个世界还没有形成网络，并不是每个人的桌面上都有一台计算机。

当然，当时对此有兴趣的只有安全部门。“安全部门对这方面的任何进展都极度重视”，瑞威斯特说，“他们竭尽所能地控制我们的方案的流传。”看起来同样的思想在情报世界紧闭的大门中早已产生，但是他们并不放心将情报人员的生命放在几位认为分解整数极其困难的数学家的手中。德国国家安全机构 BSI[①] 的安斯加·休塞尔（Ansgar Heuser），曾回忆过他们在 80 年代考虑在实际中使用 RSA 的事情。他们咨询了一些数学家是否西方的数论水平胜过前苏联的数论水平，在他们得到否定

---

① BSI 的全称为 Bundesamt für Sicherheit in der Informationstechnik。



的回答之后，这个方案就被搁浅。但是在接下来的 90 年代中，RSA 不仅证明了自己可以用来保护间谍的生命，而且可以用在商业世界之中。 231

密码卡游戏

现在，RSA 密码系统保护着因特网上绝大多数的交易。特别的是，这样的一个公钥密码系统能够成为现实，其中的数学又涉及了我们曾经讨论过的高斯的时钟计算器，以及阿德曼的偶像费马曾经证明过的一个定理——费马小定理。

在高斯的时钟计算器上的加法，是我们都熟悉的关于 12 小时时钟的加法。我们知道，九点过后 4 小时是一点。这就是时钟计算器加法的原理：将数相加，然后取除以 12 后得到的余数。和两百多年前高斯的记法一样，这个过程可以写作：

$$4+9=1\ (\text{modulo } 12)$$

时钟计算器的乘法或者方幂也是相同的原理：先在普通计算器上计算出结果，然后除以 12 取余数。

高斯知道时钟计算器并不仅仅对 12 小时的时钟有效。在高斯明确用公式写出时钟算术之前，费马就已经做出了一个很重要的发现，它被称为费马小定理。这是关于一个具有素数刻度（比如说 p）的时钟计算器的定理，如果你取一个数，并作它的 p 次方，那么得到的结果还将是原先的这个数。例如我们在一个刻度为 5 小时的时钟上，取 2 的 5 次方，其结果为 32，这个结果在刻度为 5 的时钟计算器上就是 2。当费马每次乘以 2 的时候，可以看出时钟上指针的运动其实显示出了某种规律，经过 5 次移动之后，指针会回到起点准备下一次的循环。

2 的方幂	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
普通计算器的结果	2	4	8	16	32	64	128	256	512	1024
刻度为 5 的时钟计算器的结果	2	4	3	1	2	4	3	1	2	4



如果我们取一个刻度为 13 的时钟，对 3 的方幂进行同样的计算，从 3^1，3^2 直到 3^{13}，我们可以得到

3，9，1，3，9，1，3，9，1，3，9，1，3

这一次指针并没有指向时钟上每一个刻度，但是它仍然存在着一个循环模式，当我们将 3 自乘 13 次之后，我们再次得到了 3。无论费马怎么选取素数 p 的值，总是会发生同样的事。利用高斯关于时钟算术（或称为模算术）的记号，费马实际上是发现了对于任意的素数 p，刻度为 p 的时钟上任意的起始时间 x，有

$$x^p = x (\text{modulo } p)$$

费马的发现就是那种使得数学家心跳加速的东西。究竟是什么东西使得素数能产生这样的魔法？不满足于实验观察的结果，费马希望能够证明，无论是什么样的素数，都不会令自己失望。

费马小定理出现在费马于 1640 年写给好友伯纳德·弗兰尼克·德贝西（Bernard Frenicle de Bessey）的信中，而不是某本书的空白之处，像费马大定理那样宣称已经得到了证明。不过与费马大定理一样，由于证明太长不便于在信中详细陈述。除了承诺会给德贝西寄一份证明之外，费马一直没有公开这个定理的证明过程。我们不得不在等了 100 多年之后，才见到完整证明的再次出现。在 1736 年，欧拉发现了为什么在素数刻度的时钟之上，指针总是在自乘素数次之后又回到原先的起点。同时，欧拉还将费马的结果推广到具有刻度 N（其中 $N = p \times q$，是两个素数的乘积）的时钟之上。欧拉发现在这样的时钟上，规律将在 $(p-1) \times (q-1) + 1$ 次之后出现。

在瑞威斯特参加完命中注定的那次逾越节宴会之后，在他脑中盘旋的正是费马发现的这个关于素数时钟的奇妙性质，以及欧拉对此进行的推广。瑞威斯特明白自己可以利用费马小定理作为这个数学密码的关键，令信用卡号码神奇地消失以及再现。

将信用卡号码加密类似于纸牌游戏的开始。但是这与普通纸牌不一



样，这副纸牌的数量非常巨大，你需要用100多位的数字来表示这个数量。顾客的信用卡号码就是其中的一张纸牌，顾客将自己的纸牌放在这副牌的最上方，网站则将这些牌打乱，于是顾客的那张牌看上去已经消失在海量的纸牌之中。从如此多的纸牌中找出那一张牌，对任何黑客而言都是不可能的任务。然而，有了费马小定理，网站可以用一个巧妙的方法，经过再次的洗牌之后，将顾客的纸牌洗回整副牌的最上方。这个第二次的洗牌方式就是只有拥有网站的公司知道的私钥。

瑞威斯特用来设计密码的数学十分简单，利用数学计算就可以完成洗牌的过程。当顾客在网站上下订单时，计算机获得了顾客的信用卡号码，并对其进行计算。这个计算过程是很容易完成的，但是在不知道私钥的情况之下逆向实现这个计算过程则是几乎不可能的。因为这样的计算并非基于普通的计算器，而是在高斯的某个时钟计算器上完成的。

当顾客在网站上下订单的时候，网络公司告诉他们该使用刻度为多少小时的时钟计算器。首先取两个很大的素数 p 和 q，大概都是60位左右的数字，将它们相乘得到第三个数 $N=p\times q$，这个代表时钟刻度的数将会变得很大，大概是120位左右的数字，每个顾客都用同样的时钟计算器来加密自己的信用卡号码。而这套密码的安全性就在于网络公司可以在数月之内使用相同的时钟刻度，直到他们觉得需要更换这个数字为止。

网站选择的时钟计算器的刻度数字其实就是选取公钥的过程，虽然 N 是一个公开的数，但 p 和 q 却是保密的，它们是解开加密后的信用卡号码的关键。

下一步，每个顾客收到第二个号码 E，称为加密数。对每个顾客而言，这个数 E 与时钟计算器的刻度 N 一样，也是公开的数字。为了加密自己的信用卡号码 C，每个顾客需要在网站提供的时钟计算器上计算 C 的 E 次方。（设想一下，E 就是魔术师为了打乱你所选的纸牌而需要洗牌的次数。）而最后的结果，用高斯的记号表示就是 C^E（modulo N）。



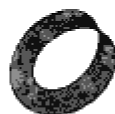
为什么说这样就是安全的？毕竟，那些游荡在网络空间中的黑客可以看见加密过的信用卡号码，以及网站公开的公钥，其中包括时钟计算器的刻度 N 和信用卡的方幂 E。为了破解这个信用卡号码，黑客们只需要找到一个数，它在刻度为 N 的时钟计算器上自乘 E 次之后，所得的结果为加密后的信用卡号码。但是要做到这一点是极其困难的，这个困难来自于时钟计算器上的方幂计算。在通常的计算器上，方幂的结果是与我们进行乘法的次数成比例的；但是在时钟计算器上就不可能发生这种情况。在时钟计算器上，你很快就会失去初始值的踪迹，因为答案的大小和初始值没有任何关系。在经过 E 次洗牌之后，黑客就会完全不知所措。

234

如果黑客试图对时钟计算器所有可能的刻度都进行计算呢？那他仍然没有丝毫机会，加密员现在使用的时钟，其表面刻度数 N 已经超过了100 位——也就是说，时钟上的刻度比整个宇宙的原子数还要多。（相比较而言，加密数 E 就很小了。）那么既然这个问题无法破解，网络公司又如何恢复顾客的信用卡号码呢？

瑞威斯特知道，费马小定理保证了存在一个奇妙的解密数 D。当网络公司将加密后的信用卡号码自乘 D 次之后，原先的信用卡号码将会再现。同样的道理也出现在魔术师的纸牌魔术中，在一定次数的洗牌之后，看上去所有的牌都已经完全被打乱，但是魔术师知道再经过一系列的洗牌过程，整副牌又将恢复它原先的顺序。比如说，标准洗牌方式——将整副牌对半分开，将两叠牌张张交错插到一起——在重复进行 8 次之后，整副牌又将回复原来的顺序。当然，魔术师的技术必须保证自己能够连续进行 8 次完美的标准洗牌。瑞威斯特正是利用了费马的技巧实现了 RSA 中的解密问题。

虽然你的信用卡号码在网站进行的一系列洗牌操作之后，已经消失在巨大数量的纸牌之中，但是网络公司知道再进行 D 次洗牌操作，就可以像魔术那样重新令你的信用卡号码回到纸牌的最上层。问题是，只有



你知道了秘密素数 p 和 q 之后，才能得到解密数 D。瑞威斯特利用了欧拉对费马小定理的推广，这适用于时钟计算器的刻度由两个素因子构成的情况。欧拉已经证明，在这样的时钟上规律将会在 $(p-1)\times(q-1)+1$ 次洗牌后出现。因此要想知道在刻度为 $N=p\times q$ 的时钟之上究竟需要多久才能出现重复规律的唯一方法就是知道素数 p 和 q，这两个素数成为解开 *RSA* 秘密的关键。只要网络公司将素数 p 和 q 置于秘密之地，那么恢复信用卡号码所需要的洗牌次数将只有网络公司自己知道。

虽然 p 和 q 必须保持隐秘，但是它们的乘积 $N=p\times q$ 却可以公之于众。因此，瑞威斯特的 *RSA* 编码的安全性就是依赖于将整数 N 分解的困难性。黑客们面对的问题也就是上世纪初科尔教授所面对的问题：找到数 N 的两个素因子。

235

摧毁 RSA 129 的盔甲

为了说服商业界分解整数这个难题有着相当的历史，MIT 三剑客引用了数学大家高斯曾经就分解问题说过的话："为了科学的尊严，我们应该想尽一切办法来解决这样一个如此一流、且如此著名的问题。"虽然高斯知道分解问题的重要性，但他在此问题上并没有什么进展。如果像高斯这样伟大的数学家都无法攻克这个问题，因此 RSA 足以保护商业公司的安全。

在他们三人将分解整数问题引入编码之前，除了高斯对 RSA 密码系统的"认证"，这个问题一直落在数学的边缘地带。大部分数学家对分解整数的细节很少关注，如果需要用一生的时间来找到大整数的素因子，那在理论上显然是毫无意义的。但是由于瑞威斯特、沙米尔和阿德曼的发现，分解问题获得了比科尔那个年代更多的关注。

那么将一个整数分解为素因子究竟有多么难？当年的科尔没有电子计算机的协助，因此他花了许多个星期天来得到梅森数 $2^{67}-1$ 的两个素

因子193 707 721和761 838 257 287。有了现代的计算机，是否我们就可以利用它一个一个尝试找到能够整除我们的目标整数的因子呢？问题在于，要想分解100位以上的整数，我们需要检查的整数个数将比可见宇宙中所有粒子的个数还要多。

由于有这么多的数需要检验，瑞威斯特、沙米尔和阿德曼有了足够的信心提出一个悬赏：将一个129位整数分解为两个素因子。这个数以及一段加密信息，出现在马丁·加德纳在《科学美国人》那篇将RSA密码告诉全世界的文章中，代号为“RSA 129”。由于他们三人当时还未成为百万富翁，因此成功找出“RSA 129”的两个素因子的人，将获得他们三人提供的100美元奖金。在文章中，他们估计将需要4×10^{16}年才有人破解“RSA 129”，但是不久他们发现自己在估算时间的时候犯了一个算术错误。尽管如此，考虑到当时已有的分解整数的技巧，破解“RSA 129”仍然需要数千年。

236

RSA使得编码者的梦想成为了现实：不可破解的密码。由于有如此多的素数需要检验，因此可以合理地认为这个系统不可破解。德国人也曾经以为，由于Enigma密码的可能组合比宇宙中的星星还要多，所以该密码坚不可摧——但是布莱切利的数学家表明，不能总是将信心放在大数之上。

“RSA 129”的盔甲最终被摧毁。没有人回避这个挑战，全世界的数学家都为此努力工作。在随后的几年中，他们发明了许多方法来找到瑞威斯特、沙米尔和阿德曼的两个秘密素数。结果，并没有需要三位数学家预测的4×10^{16}年，仅仅只用了十七年，这个数就被成功分解。即使是这样的时间，也足够保证经过“RSA 129”加密的信用卡在过期之前不被破解。随之出现的问题就是，数学家究竟需要多久才能想出一个新的方法，将十七年缩短为十七分钟。

新的分解技巧

密码学和数学之间的互动，将现代数学家带入一种新的、更像是实



验和实践科学的文化中。自从19世纪德国学校从大革命法国数学家手中接过接力棒以来，这种文化就从未被体验过。法国数学家认为自己的学科是实践的工具，只是一种手段而已；而德国的洪堡则相信对知识的追求是为了知识本身。很快，那些仍然坚持德国传统的理论数学家谴责分解整数的研究，用亨德里克·兰斯特拉（Hendrik Lenstra）的话来说，是“玫瑰花园中的一头猪”。相比于追求严密的证明，这样的素数问题被认为是不重要的工作，因此也没有什么数学家关注。但是当RSA密码系统在商业上越来越重要时，找到一个有效的方法，求出隐藏在大整数背后的素数因子，就变得不可避免。渐渐地，越来越多的数学家被吸引到破解RSA 129的挑战中。最终的突破得益于更快计算机的出现，更重要的则是意料之外的理论上的进展。为了破解这个密码而产生的新问题同时也导致了一些更深层次数学的发展。 237

卡尔·波莫伦斯（Carl Pomerance）也是被这门新兴学科吸引的数学家之一。波莫伦斯将自己的时间分为两部分，一段用于佐治亚大学的学术工作，另外一段则用在新泽西贝尔实验室中进行商业研究。作为一个数学家，他拥有孩童般对于数字的兴趣，并希望能找到其中的新联系。波莫伦斯对于棒球比分数字的研究论文引起了厄多斯的兴趣，这位匈牙利人注意到了他以及他论文中提出的一些有趣问题。在没有提前通知的情况下，厄多斯到佐治亚访问了波莫伦斯，两人合作写出了20多篇文章。

波莫伦斯对于分解整数的兴趣来自于高中数学竞赛。当时有一道题要求分解8051，并要求在5分钟之内完成，而当时还没有微型计算器。虽然波莫伦斯长于心算，但他决定首先看看，是否可以找到一个巧妙的捷径，而不是通过一个一个尝试来找到答案。“我用了两分钟左右寻找新方法，逐渐地我觉得自己浪费了太多时间，我开始变得焦急，于是重新开始尝试可能的因子，但由于时间浪费太多，我没有做出这道题。”

分解8051的失败，激起了波莫伦斯一生对于快速分解整数方法的



研究，最终他学会了高中老师教授的技巧。在1977年之前，分解整数最有效的办法仍然来自费马，他的小定理曾经是发明RSA素数密码系统的催化剂。利用某些简单的代数知识，费马分解方法对于某些特别选定的数非常有效。利用费马分解方法，波莫伦斯只用了不到一分钟就将8051分解为83×97。曾经热爱加密理论的费马，如果能看到自己的思想在3个世纪之后，成为破解密码的核心方法时，也会感到很欣慰。

当波莫伦斯听说了瑞威斯特、沙米尔和阿德曼的悬赏之后，他立刻就意识到，如果能将这个129位的整数分解，那么将能驱散自己童年失败的回忆。在20世纪80年代初，他逐渐感到肯定有某种方法可以利用费马分解方法，将费马分解方法应用到不同的时钟计算器上，就可以构成一台强大的分解机器。现在高中数学竞赛已经不再是他的目标。这个新发现被称为“二次筛选法”，它在新兴的因特网安全方面有着非常重要的应用。

波莫伦斯的二次筛选法利用了费马分解方法。在实际应用时，它连续地改变时钟计算器的刻度，对目标整数发起攻击。这个方法类似于亚历山大的图书管理员埃拉托塞尼发明的埃拉托塞尼筛法（sieve of Eratosthenes），通过依次选取素数来删去那些是该素数倍数的合数。因此通过不同大小的筛，就可以将那些合数（非素数）统统消灭，而不需要单独考虑它们。在波莫伦斯用来进攻素数的筛法中，不同刻度的时钟计算器可以看作不同的筛，不同的时钟计算器计算得到的结果，都会给波莫伦斯更多关于可能因子的信息，使用的计算器越多，波莫伦斯离整数分解为素因子的目标就更近一步。

238

这个思想的最终考验就是完成RSA 129的挑战。但是在20世纪80年代，波莫伦斯的分解机器对这个大数仍然无能为力。到了90年代初期，因特网的发展帮助了波莫伦斯，两位数学家阿仁·兰斯特拉（Arjen Lenstra）和马克·玛纳斯（Mark Manasse）意识到因特网将会成为利用二次筛选法攻克RSA 129的最好助手。因为波莫伦斯的方法有一个优



点，就是可以利用不同的计算机分担整体的工作量。通过分配不同的任务到个人计算机上，因特网曾被用来寻找梅森素数。玛纳斯和兰斯特拉觉得可以通过分配不同的时钟计算器到个人计算机上，来合作攻克 RSA 129。本来由这些密码系统保护的因特网，现在则被用来协助攻克 RSA 129 的挑战。

兰斯特拉和玛纳斯将波莫伦斯的二次筛选法放到网上招募志愿者加入。1994 年 4 月，集合了 24 个国家数百台计算机的威力，加上 8 个月的实时计算终于破解了 RSA 129。这一计划的领导者是 MIT 的德雷克·阿特金斯（Derek Atkins）、爱荷华州立大学的麦克尔·格拉夫（Michael Graff）、牛津大学的保罗·利兰德（Paul Leyland）和兰斯特拉。甚至两台传真机也加入了这个计划——当它们没有在传递信息时，分别被用来检查两个 65 位和 64 位的素数。该计划最终使用了 524 339 个不同的素数时钟计算器。

在 20 世纪 90 年代后期，瑞威斯特、沙米尔和阿德曼又提出了一系列新的挑战。直到 2002 年底，这些挑战中最小的、一个 160 位的数仍然没有被攻克。由于三人的财富比 1977 年有了大幅提高，因此如果你破解了这些数，就可以得到 1 万美元的奖励。瑞威斯特销毁了用来生成这些大整数的素数，这样在真正破解之前就没有人知道这些素数。RSA 信息安全公司（RSA Security）认为 1 万美元是让自己领先于那些数字攻克者的代价，每一次他们得到了新的纪录，RSA 就可以建议商业公司增加素数的大小。

239

波莫伦斯二次筛选法的继任者是数域筛选法。这个新的筛选法保持着现今的纪录，它破解了 RSA 155。这是一些数学家在名为“卡巴拉”（Kabalah）计划下合作取得的成果。破解 RSA 155 是心理上的巨大突破，因为在 20 世纪 80 年代中期，安全机构还没有重视 RSA 思想的时候，这样的复杂程度对于计算机安全而言已经足够。现在，正如德国安全机构 BSI 的安思伽·休塞尔（Ansgar Heuser）在伊森举办的一次密码



会议上承认，如果他们没有事先考虑到这一点，现在“将会是一场灾难”。目前，RSA 信息安全公司推荐使用的时钟计算器的刻度 N 至少为 230 位；而像 BSI 之类的情报机关，为保护情报人员的长远考虑，将使用超过 600 位的数作为时钟计算器的刻度。

埋在沙中的脑袋

数域筛选法在好莱坞电影《通天神偷》（*Sneakers*）中曾经露过一次面。罗伯特·雷德福（Robert Redford）坐着听一位年轻数学家谈论如何分解大整数的问题：“数域筛选法是目前已知最好的方法。当然也可能存在着更好的方法……但是也许，仅仅是假设，这里有一条捷径……”毫无疑问，这位由多那尔·罗格（Donal Logue）饰演的小专家肯定发现了某种方法，“一个高斯比例的突破”，并且在一个小盒子中实现了它。不幸的是，这个盒子落入了由本·金士利（Ben Kingsley）扮演的坏人手中。电影的场景非常古怪，大多数看过电影的人认为这根本不会在现实中发生。然而，在电影最后滚动的演职员表中，你可以发现“数学顾问：阿德曼”，正好是 RSA 中的 A。阿德曼承认，我们不能保证这个场景一定不会发生。《通天神偷》的编剧拉里·拉斯卡（Larry Lascar）（他也写过 *Awakening* 和《战争游戏》）拜访了阿德曼以确保电影中的数学不会出错。“我喜欢拉里和他对真实性的追求，因此我同意担任数学顾问。拉里希望付给了我报酬，但是我用雷德福来交换——如果让我的妻子萝莉和雷德福见一次面，我就做顾问。”

商业界是否已经对这样的学术突破做好了准备？一些企业具有前瞻性的目光，但是大部分企业仍然将脑袋埋在沙中。如果你问商业机构和政府安全部门，他们的答案会稍微令人担心。下面是我在密码协会中记录下来的一些发言：

“我们已经符合了政府标准，这是我们最关心的事。”



"如果我们失败了,至少会有一大帮人跟着我们一起失败。"

"希望在这样的数学突破出现之前，我已经退休了，这样就不关我的事了。"

"我们按照理想的原则工作——暂时没有人能做出巨大的突破。"

"没有人可以给出保证。我们同样不希望如此。"

当我给商业界做因特网安全的演讲时，我总喜欢提出自己的 RSA 悬赏：最先找出 126619 的两个素因子的人将得到一瓶香槟。我在全世界三个不同的地方为银行业演讲时得到了不同的回应，它们反映了商业世界对待安全问题的不同文化差异。在威尼斯，欧洲的银行家根本没有把这个悬赏和密码背后的数学当一回事，我只好依靠听众中的间谍来帮我完成这个挑战。与欧洲的银行家相对比，具有良好人道主义教育的远东银行家显示出了更好的科学修养。在巴厘岛的演讲结束时，一位男子站起来告诉我那两个素数，从而赢得了香槟。比起欧洲的对手，远东的银行家能够更好地欣赏数学及其在电子商务中的应用。

在对美国人做的演讲中，我得到最深刻的印象。在我演讲后回到休息室不到 15 分钟的时间里，我接到了三个正确答案的电话。其中两位美国银行家登录到因特网上，下载了破解程序来计算 126619；第三位则没有透露他的方法，我怀疑他是偷听了前两位银行家的结果。

商业界将它的信任放在了一部分数学上面，但是只有很少人愿意花时间亲自检验。没错，正是由于这些马虎的管理者将重要信息不加保密放在网站上，才导致了每天网络商业安全面对的威胁。和任何密码系统一样，RSA 极易受到人类缺点的影响。在第二次世界大战中，由于德军操作员编制的密码手册中含有大量错误，盟军才能得益于此，并最终破解了 Enigma 密码。同样，如果网络操作者选择极易破解的数字作为密码，RSA 也同样可以被破解。如果你希望破解密码，那么买一台二手的计算机，与花费心思去获得一个纯数学的博士学位，前者的投资更划算。因为大量留在过时机器上的敏感信息也许会对你有所帮助。另外，

241

简单贿赂掌管着密钥的人所得到的回报，也许比你赞助一组数学家破解密码得到的回报要多得多。就像布鲁斯·施内尔(Bruce Schneier)在《应用密码学》中说的，"找到人的缺点比找到密码系统的缺点容易得多。"

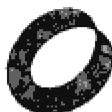
然而，尽管这些安全缺陷对具体涉及的公司而言很严重，但绝不足以影响整个因特网商业的结构。这就给《通天神偷》这样的电影留下了可以发挥的空间。尽管在破译密码方面出现突破的可能性极小，但是威胁仍然存在，并且结果也许会是全球性的灾难。它也许会像电子商务中的千年虫，让整个世界里电子邮件彻底消失。我们"认为"破解数字从本质上而言很难，但是我们无法证明。如果我们能够告诉那些管理人员不可能找到一个分解整数的快速算法，那么他们会轻松不少。显然要证明这一点同样很困难。

分解整数是一项复杂的任务。并不是因为涉及的数学很难，而是因为这件工作类似于在一个巨大的草堆中寻找两根针。还有其他很多这样涉及"草堆"的问题，比如说，虽然每一张地图都可以用4种颜色着色，那么你怎么样判断一张给定的地图是否可以只用3种颜色就能着色？唯一能够判断的办法就是费力地试遍所有可能的组合方式，如果你足够幸运，你就可以用3种颜色给这幅地图着色。

兰登·克莱的千禧年问题之一是P与NP问题，它主要考虑的就是这一类有趣的问题。如果一个问题的复杂性像分解整数或给地图着色那样需要搜寻大量的可能途径，那么是不是总存在一种有效的方法可以找到这根针？我们的直觉告诉我们P与NP问题的答案是否定的，即存在着某些问题，即使当代高斯的技巧也不能处理它们内蕴的复杂性。但是如果这个问题的结果是肯定的，瑞威斯特说，"这将是密码界的灾难。"大部分的密码系统，包括RSA考虑的都是关于巨大草堆的问题，千禧年问题的肯定回答意味着存在某个快速算法来分解整数——只是我们现在还不知道而已！

242

数学家希望构建我们数学大厦的基石具有百分之百的安全性，而商业界对此并不太关心。这一点毫不奇怪，因为分解整数看上去在最近仍



然保持着它的难度，商业世界也乐于在安全性为99.99%的地基上进行他们的网络商业。大部分数学家认为在分解整数这个问题上有着天然的计算难度，但是没有人能预测在未来10年中会有什么进展，毕竟RSA 129也只坚持了不到20年的时间。

分解整数问题如此困难的原因之一是素数的随机性。由于黎曼假设正是试图去理解素数无序行为的源头，因此黎曼假设的证明也许会为我们提供一些新观点。1900年，希尔伯特在描述黎曼假设时曾强调黎曼假设的解答拥有解开更多数之秘密的潜力。由于黎曼假设在理解素数方面的中心地位，数学家推测，如果找到了黎曼假设的证明，也许能为分解整数提供一些新的途径。这也正是为什么商业界总是关注着素数研究的原因。商业界对黎曼假设情有独钟的另外一个原因是，在他们利用RSA密码系统加密之前，他们必须先找到两个60位的素数，如果黎曼假设正确，那么就会存在一个寻找素数的快速方法，从而可以构造出更多RSA密码，保障电子商务的安全。

寻找大素数

由于因特网的快速发展以及随之而来的对越来越大的素数的需求，让欧几里得关于存在无穷多素数的证明突然获得了意想不到的商业上的重要性。如果素数是这样难以驾驭的东西，那么商业界如何找到这些大素数呢？事实上确实存在着无穷多个素数，但是当我们越往大数的方向走，素数就越稀少。如果我们走得更远，那么是否有足够多的60位素数来满足世界上的每个人，使他们都能得到两个来构成他们自己的私钥？即使有足够的素数，如果它们是仅仅足够，那么在这种情况之下，两个人得到同样一对素数的几率就会变得很大。

幸运的是，自然界对电子商务很仁慈。高斯的素数定理告诉我们60位的素数个数大概是10^{60}除以10^{60}的对数，这意味着存在足够多的60位的素数，以至于地球上每个原子都可以分到自己的一对素数。不仅如此，

243



你赢得国家彩票的几率都要大于两个不同原子获得相同一对素数的几率。

因此，我们知道存在着足够多的素数可供选择，那么我们如何知道某个数是素数呢？我们已经知道，对于一个非素数的整数，找出它的素数因子是一件相当困难的事。如果一个候选整数本身就是素数，那么验证的过程是不是要加倍的艰难，因为你必须证明没有更小的数整除这个候选整数。

最终结果表明决定一个数是否是素数并非像我们想象中的那么困难。即使你无法找到候选整数的素因子，也存在着一种快速检测法来判定某个整数是否为素数。这也就是为什么在科尔教授分解那个大整数之前 27 年，数学界就知道这个数不是一个素数。不过这个检验对于预测黎曼假设所关心的素数分布并没有太大的帮助，但由于它可以告诉我们某个特定的整数是否为素数，因此它帮助我们听到了素数音乐中的单个音符，尽管它不能帮助我们欣赏黎曼假设描述的那首完整的旋律。

这个检测方法同样来源于费马小定理，瑞威斯特在逾越节宴会那晚发明 RSA 加密系统的时候，费马小定理也曾登场。费马发现，如果在一个刻度为素数 p 的时钟计算器上任取一个数，然后求出它的 p 次方，最后的结果就是这个数本身。随后欧拉因此意识到费马小定理可以用来证明一个数不是素数。比如说，在一个刻度为 6 小时的时钟计算器上，将 2 连续自乘 6 次，结果指在 4 点。如果 6 是素数，我们应该可以回到 2 点，因此由费马小定理可知 6 不是一个素数——否则这就是费马小定理的反例。

如果我们想知道一个数 p 是否为素数，我们可以取一个刻度为 p 的时钟计算器，然后测试不同的时间，看看它们在自乘 p 次之后是否回到原先的出发点。只要无法回到原出发点，我们就可以将这个数丢掉，因为它肯定不是素数。如果每一次的时间都满足费马检验，那么我们根本不需要去证明 p 是一个素数，因为时钟上的每一个刻度都会为 p 的素数宣言作证。



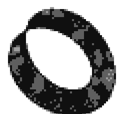
为什么在时钟计算器上进行验证要比验证每个小于 p 的数是否能整除 p 更好？其关键在于，如果 p 无法通过费马检验，那么这种情况非常明显，时钟上超过一半的数都无法通过费马检验，从而可以证明 p 的非素数性。因此有许多种途径证明这个数不是素数，这是重大的突破，它与通过验证每个数是否为 p 的因子这样的逐步除法检验形成了鲜明的对比。如果 p 是两个素数的乘积，那么在所有的除法中仅仅只有这两个素数能证明 p 不是素数，而其他任何数对结果都没有帮助。如果要让逐步除法检验成功，你必须正确地挑中那两个素数。

244

在众多的合作成果之中，厄多斯估计（虽然没有给出严格证明）要判断一个小于 10^{150} 的数是否为素数，只要在时钟计算器中找到一个可以通过费马检验的时间，就意味着该数不是素数的可能性小于 $1/10^{43}$ 分之一。《素数纪录》（*The Book of Prime Number Records*）一书的作者保罗·瑞本波（Paulo Ribenboim）指出，利用这个检测，任何贩卖素数的机构都可以在卖出商品时打出"保证满意，无效退款"的横幅，而不用担心破产。

数百年来，数学家将费马检验作了进一步的完善。在 20 世纪 80 年代，两位数学家盖瑞·米勒（Gary Miller）和麦克尔·拉宾（Michael Rabin）终于得到这个检验的一个改进，可以保证只需经过数次检验就能确定一个数是否为素数。但是米勒-拉宾检验有一点不确定：这个检验对于大数的效果依赖于黎曼假设的证明。（准确地说是黎曼假设的一个推广。）这也许是我们知道的藏在黎曼峰背后的最重要的结果。如果你能证明黎曼假设及其推广，那么除了可以得到 100 万美元，你还能保证米勒-拉宾检验是证明一个数是否为素数的最快且最有效的方法。

在 2002 年 8 月，坎普尔印度理工学院的三位印度数学家马林德拉·阿格拉瓦（Manindra Agrawal）、尼拉贾·卡亚尔（Neeraj Kayal）和尼廷·萨克赛纳（Nitin Saxena）找到了米勒-拉宾检验的一种替代方法。这种方法比原方法要慢，但是避免了黎曼假设成立的前提。这绝对是素数领域的一大惊喜，在坎普尔传出消息的 24 小时之内，全世界有超过 3 万人——其中也包括了卡尔·波莫伦斯——下载了这篇文章。这篇文章



内容十分清晰易懂，当天下午波莫伦斯就在讨论班上向自己的同事们介绍了其中的详细内容，波莫伦斯认为他们的方法“惊人的奇妙”。拉马努扬的精神仍在印度传承，这三位数学家并不害怕挑战已知的该如何检验一个数是否为素数的结论。他们的故事给我们提供了信心，也许某天某个不知名的数学家突然出现，带着自己的思想最终解决了黎曼假设，这个终极的素数问题。

245

由此看来，自然界对于密码学界是多么的仁慈。她提供了一种快速并且简单的方法生成因特网密码系统所需的素数，同时整数分解为它的生成素数的快速方法又被她隐藏起来。但是自然界究竟会站在加密者一方多久呢？

未来的椭圆，未来之光

素数理论在商业核心问题中的应用大大地提升了数学的地位。如果有人质问资助像数论这样深奥的领域到底有什么用，那么指出素数在 RSA 中的地位应该是一个有力的回击。菲尔兹奖获得者迪默西·高尔斯（Timothy Gowers）在克莱千禧年问题的发布会上所作“数学的重要性”报告中就引用了这样的一个例子。

在这个新的加密方法出现之前，大部分数学家手头上都缺少一个像这样引人注目的抽象数学的应用。可以说这是该领域幸运的也是及时的突破，你可以在任何有关数论的研究经费申请书中写上“也许会有密码学方面的应用”这样一句流行语。公正地说，RSA 密码系统背后的数学并不高深，大部分数学家不会将分解整数的挑战与解决那些像黎曼假设一样长期存在的难题去相比。

虽然像黎曼假设或 P 与 NP 问题的结果都会对 RSA 产生影响，但却是另外一个千禧年问题差点引发电子商务的千年虫灾难。早在 1999 年就迅速流传着一条传言，说某个被称作伯彻-斯威那顿-戴尔猜想（Birch-Swinnerton-Dyer Conjecture）、关于椭圆曲线的问题有可能暴露因



特网安全的阿喀琉斯之踵①。

1999 年 1 月《泰晤士报》登出一篇头版文章，标题是“少女破解电子邮件密码”。这项成就为爱尔兰少女萨拉·弗兰娜瑞（Sarah Flannery）获得了一项科学竞赛的奖励，但这离富有还很遥远。文章所配插图是女孩站在一块引人注目的满是数学式子的黑板前面，插图标题说，“萨拉·弗兰娜瑞，16 岁，她用自己掌握的密码学击败了裁判。他们认为她的工作是‘很出色的’。”由于因特网对“电子邮件密码”的依赖性，这篇文章抓住了媒体和公众的兴趣。进一步阅读下去，可以知道这个标题并不是指对 RSA 安全性的一种新的攻击方式，但是一个实际问题的答案却影响到了 RSA 密码系统的应用。

246

利用 RSA 加密或解密信用卡号码的过程，就是将这个号码在一个刻度为上百位数的时钟计算器上自乘许多次。计算这样大的数字需要占用计算机相当长的时间。大部分网站并不仅仅询问你的信用卡号，他们有时还会询问你的更多信息，然后他们利用 RSA 系统决定一个私钥，用来在你的电脑上和网站上对这些信息进行加密。由发送者和接收者共同拥有的私钥，其加密过程比 RSA 公钥的加密过程快很多。

如果你在自己家中，利用具有大容量内存和高速 CPU 的个人电脑进行网上购物，那么你根本不会觉察到加密信用卡号码的时间。然而逐渐地，我们可以在家庭以外的地方接入因特网，移动电话、掌上电脑以及在未来会出现的其他手持设备都具有网上冲浪的能力，被称为 3G（third-generation）的科技为这些设备在因特网上的通讯提供了途径。但是当你完成网络选购，涉及在一台掌上终端进行信用卡加密的时候，这种小型手持电脑的能力就被推到了极限。

移动电话和掌上电脑并非为大型计算而设计，它们与你的桌面计算机相比，只有有限的内存和慢得多的处理器。不光如此，这些移动设备

① Achilles' heel，阿喀琉斯是希腊神话中的英雄，是珀琉斯和西蒂斯之子，传说他除脚踵外全身刀枪不入。

用来传送信息的网络带宽也比电话线或网线要窄，因此将传输数据压缩到最小是必要的。为了保证自己的系统永远领先于更快的用来破解的计算机，RSA 系统需要的大整数在不断地增大，因此 RSA 并不适合于移动设备有限的能力。

多年来，密码设计者一直在追寻一种新的公钥密码系统，它的安全性和使用范围不亚于 RSA，但是比 RSA 更小并且更快速。1999 年，《泰晤士报》以及其他媒体就接受了这样的可能性，16 岁女孩萨拉·弗兰娜瑞发现的正是我们需要的新密码系统。弗兰娜瑞的密码确实很快，但是6 个月之后有人在其中发现了漏洞，从而表明这样的系统并不安全。这个故事对商业世界而言是一个善意的警告，因为某些公司已经打算投资弗兰娜瑞的新密码了。值得赞扬的是，弗兰娜瑞本人从没有宣称该密码是安全的。要证实安全性只有靠时间和测试——媒体根本没有意识到这两者。最后证明过于仓促地提出这个密码反而揭露了某些幕后操纵者。

247

但是 RSA 确实面对着一位竞争对手，并且这位竞争对手符合移动世界、无线通讯或移动商业的挑战。在这种新的密码系统背后不是素数，而是某种更加奇怪的东西：椭圆曲线。这些曲线由具有特殊形式的方程所定义，并在安德鲁·怀尔斯关于费马大定理的证明中处于核心地位。它们已经作为一种快速的将整数分解为素数的方法进入了密码学世界，好像这正是一条不成文的规定，密码破解者用更好的编码系统对密码制造者发出了反击。华盛顿大学西雅图分校的尼尔·柯布利兹（Neal Koblitz）正在研究利用椭圆曲线来破解密码，同时他也注意到椭圆曲线同样可以等价地用来生成密码。柯布利兹在 20 世纪 80 年代中期提出椭圆曲线加密法，与此同时，新泽西拉玛坡学院（Ramapo College）的维克多·米勒（Victor Miller）也发现了如何由椭圆曲线编制密码。虽然这些密码比 RSA 都要复杂，但是基于椭圆曲线的密码系统不需要如此大的数字作为密钥——因此非常适合于移动商务。

尽管柯布利兹由于自己发明的密码系统适用于移动设备而被卷入商



业世界，但对他而言，他的心仍然在哈代所谓的纯数论世界中。作为数论界的一位资深数学家，柯布利兹仍保持自己对数学的热情，那是由童年时期意外发生的一连串偶然事件引起：

> 当我6岁时，我们全家在印度的巴罗大（Baroda）呆了一年，那里学校对数学的要求比美国的要高许多。第二年当我返回美国时，我已经超过同班同学一大截，我的老师误认为我对数学有特殊天分。就像其他一些容易在老师头脑中形成的错误概念一样，这种错觉逐渐变成了一种自我实现的预言。我从印度回来之后受到的所有鼓励，促使我走上了数学家的道路。

柯布利兹早年在印度的生活不光对他的数学发展贡献良多，而且还促使他认识了世界社会的不公平。作为一个成年人，他加入了支援越南和中美洲的数学计划；在他众多关于数论和密码学的书籍中，有一本是“纪念那些为抵抗美国侵略战争而牺牲的我的越南、尼加拉瓜和萨尔瓦多的学生”，这本书的收益都用于购买赠送给这三个国家人民的书籍。

248

在国内，柯布利兹抗议美国政府国家安全局对数学领域设下的束缚。现在某项关于数论的工作在发表之前都必须得到国家安全局的授权，即使是在最深奥的数学杂志上。由于柯布利兹的新思想，有关椭圆曲线的研究工作和素数一样，成为了“被禁止名单”中的一员，处于政府的密切注视之下。

瑞威斯特、沙米尔和阿德曼利用高斯的时钟计算器来打乱信用卡账号，柯布利兹则希望利用奇怪的曲线让你的信用卡号消失不见。与时钟计算器上的乘法不同，柯布利兹希望使用一种定义在曲线中的点之上的奇怪乘法。

迦勒底诗的乐趣

起初，RSA觉得这位街头新来的密码系统对自己形成了威胁，这是



对它们在因特网密码系统垄断地位的挑战。1997 年，RSA 的不安达到了顶点，当时他们新开了一个叫做 ECC Central 的网站。在这个网站上张贴着一些著名数学家和密码学家关于怀疑椭圆曲线是否具有它所宣称的安全性的言论。有人说分解整数具有非常悠久的历史，可以一直追溯到高斯的那个年代，如果高斯也解决不了这个问题，那么你的安全性肯定可以得到保证。还有人说，椭圆曲线的结构是如此丰富，也许能给黑客提供立足点从而可以破解这种只有小型密钥的密码系统。毕竟萨拉·弗兰娜瑞的密码系统只有 6 个月的安全期。

RSA 小组也指出，如果你向银行家解释是什么在保护他们数以亿计的交易的安全，解释整数分解问题几乎没有什么困难，但是如果你开始写下 $y^2=x^3+\cdots$，很快他们的眼光就会变得呆滞。而椭圆曲线密码系统的主要支持者 Certicom 公司在反击这些批评时说，在他们举办的商业安全课程结束的时候，银行家都很高兴地玩起了椭圆曲线上的点。

但是真正激怒椭圆曲线阵营的发言来自罗恩·瑞威斯特，RSA 中的字母 R，“评估椭圆曲线密码系统的安全性，有点像评估某些刚发现的迦勒底诗歌。”

249

ECC Central 网站开张的时候，尼尔·柯布利兹正在伯克利讲授椭圆曲线。他从来没有听说过迦勒底诗歌，于是他赶到学校的图书馆查询这个名词。在图书馆中，他发现迦勒底是在公元前 625 年至公元前 539 年统治南巴比伦地区的古代闪米特（Semitic）人。“他们的诗歌是伟大的作品，”柯布利兹说。因此他将椭圆曲线的图像和“我爱迦勒底诗歌”这一口号印上了 T 恤衫，并分发给参加讲座的听众。

迄今为止，椭圆曲线已经经受住了时间的考验，并成功地进入了国家标准。移动电话、掌上电脑和智能卡中都应用了这项最新的密码系统。你的信用卡号码被这些椭圆曲线加密，并且不留下任何痕迹。虽然最初是为小型移动设备设计，但椭圆曲线密码也逐渐成为一些大型系统的选择。德国安全部门 BSI 公开承认，现在他们情报人员的生命依赖于椭圆曲线带来的安全性。甚至不久以后，当我们乘坐飞机旅行时，我们



自己的生命就将交到这些曲线的手中，椭圆曲线即将用来保护世界上航空交通控制系统的安全。随后RSA关闭了自己的ECC Central网站，现在的RSA信息安全公司在研究自己的RSA系统的同时，也在研究椭圆曲线密码系统的应用。

然而在1998年夏天，担心椭圆曲线拥有的特殊结构也许会导致这个密码系统崩溃的想法开始萦绕在那些曾经因为相信椭圆曲线的安全性而进行投资的人心中。就在几个月前，尼尔·柯布利兹曾给出声明，关于椭圆曲线最著名的问题伯彻-斯文那顿-戴尔猜想（Birch-Swinnerton-Dyer Conjecture）也许不会对椭圆曲线在密码学中的应用产生影响。但是正如哈代关于数论永远不可能实用的预言一样，柯布利兹的预言最终报复了他自己。实际上，也许正是柯布利兹的宣言太过于挑衅，才激发了布朗大学的约瑟夫·西佛曼（Joseph Silverman）提出了一种基于伯彻-斯文那顿-戴尔猜想的攻击方法。

伯彻-斯文那顿-戴尔猜想也是7个千禧年问题之一，它希望能确定一个椭圆曲线的方程存在有限多个解还是无限多个解。在1960年，两位英国数学家布赖恩·伯彻(Bryan Birch)和彼得·斯文那顿-戴尔爵士(Sir Swinnerton-Dyer)猜想，这一结果藏在一个虚数世界中，就像黎曼发现的那个世界一样。尽管有人会误以为在这个猜想的背后有三个人——伯彻、斯文那顿和戴尔，但是由于他们的猜想，伯彻和斯文那顿-戴尔成为了(数学家心中)不可分割的两个名字，就像劳莱和哈台一样①。伯彻相当笨拙的风格与劳莱很像，而斯文那顿则像不爱讲话的哈台。

250

① Stan Laurel和Oliver Hardy是美国著名电影喜剧演员。原名Arthur Stanley Jefferson Laurel的劳莱和原名Oliver Norvell Hardy, Jr. 的哈台从1926开始合作，早期合作演出的有《让菲利普穿上裤子》(1927)等短片。他们一共合演了一百多部喜剧，包括《让他们笑去》(1928)、《音乐盒》(1932)、《沙漠之子》(1933)和《在那遥远的西部》(1937)等，公认为好莱坞第一队优秀的喜剧组合。瘦得皮包骨的劳莱通常扮演笨手笨脚、头脑简单的人物，衬托肥胖而狂妄自大的哈台，两人把一些日常小事弄得一团糟，闹的不可开交。(摘自“大英百科全书”)



黎曼发现了将你从素数带入到ζ函数世界的虫洞，而另一位哥廷根的数学家赫尔姆特·哈瑟（Helmut Hasse）则发现每一条椭圆曲线都有自己对应的虚数世界。哈瑟是德国数学历史上一位有争议的人物，在希特勒对哥廷根数学系进行大肆破坏时，哈瑟得到了纳粹的任命，负责接管数学系的日常事务。由于他对纳粹的忠诚以及他的数学能力，哈瑟成为当权者眼中合适的候选人，并希望他能保持哥廷根的传统。

数学界对哈瑟抱有复杂的感情，几乎没有人可以原谅他做出的政治选择。在1937年，他甚至写信给政府要求将自己的一位犹太祖先从记录中划去，从而可以加入纳粹党。卡尔·路德维格·西格尔回忆说，当他1938年出访回来的时候，发现"哈瑟第一次戴上了纳粹党的徽章！我对此完全不能理解，怎么这样一个有智力有理性的人会戴上这样一个东西。"抛开哈瑟的政治问题，他的数学洞察力更加知名。他的名字因为哈瑟ζ函数而永垂不朽，这个函数建立的虚数世界，正蕴涵着那些椭圆方程解的个数的秘密。

黎曼发现了如何建立包含所有虚数的完整函数世界的方法，而哈瑟对椭圆曲线世界却不能做同样的事。对每个椭圆曲线，他可以部分地构造出对应的世界，但是到达某一点之后他发现自己面对的是一道横亘南北的山脉，而他自己并没有适当的技巧能够翻越。最后正是在怀尔斯证明费马大定理的过程中，我们找到了如何穿越这个障碍并画出另一边世界的方法。

然而，在我们知道山脉那一边是否有东西存在之前许多年，伯彻和斯文那顿-戴尔就已经猜想到了这个假设的世界将会告诉我们什么。他们预测，在山脉两边的世界中各存在一个点，它们包含着用来构造这个世界的特定椭圆曲线的解是否为无穷多的秘密。其方法是在虚数世界中测量数1上方的点的高度，如果此处的点正好位于海平面，则该椭圆曲线有无穷多个局部解；另一方面，如果此处的点并不位于海平面，那么肯定只有有限多个局部解。如果伯彻-斯文那顿-戴尔猜想正确，那么这些位于两边虚数世界中的点就包含了找到椭圆曲线的解的秘密，同样这

251



也是表示虚数世界能力的另一个强有力的例子。

虽然伯彻和斯文那顿-戴尔因理论需要的激发提出这个猜想，但这个猜想更多的是来自于特定椭圆曲线的实验结果。伯彻回忆说那个灵感到来的时刻，他正在研究那些计算结果中的数字，“当时我正待在德国黑森林①地区一间美丽的旅馆中，我将得到的数字一个一个地画出来，突然发现许多点排列在四条平行线上……太妙了!”出现这些直线特征意味着存在某种强烈的关系迫使这些点排列成直线。“从那时起我就很明确肯定有东西在那里，我回去之后找到彼得，‘嘿，看看这个!’”看来这是伯彻碰到的另一件好事，“彼得说‘我早就跟你说过了’——他总是这么说。”

这个猜想于20世纪60年代提出，在此之后出现了不少重要的进展。怀尔斯和查吉尔都对此猜想做出了重要贡献，但是离最终结果还有很长一段路。它的重要性可以由被选为千禧年问题而看出，同时它也是唯一的一直有着不断进展的千禧年问题，然而伯彻相信还需要很长时间才会出现领取克莱大奖的人。但不管怎样，伯彻-斯文那顿-戴尔猜想是一张价值百万美元的通行证——并不是克莱的100万，而是依赖于因特网密码安全性的那些数以百万计的资金。

基于椭圆曲线的密码依靠的是找到某些算术问题的解的难度。约瑟夫·西佛曼知道对伯彻-斯文那顿-戴尔猜想的探索也许能提供某种方法，对密码问题进行一定程度的转换从而发现一些线索，告诉我们该到何处去寻找解。这样的可能性当然很小，西佛曼承认自己也怀疑是否存在一种有效的攻击手段，但是这种方法也许能转化为黑客们正在渴求的那种快速程序，没有专家能轻易地否认这一点。

如果这个攻击方法被公布于众，西佛曼将会成为公众人物；媒体将会陷入疯狂状态；RSA 则在一旁沾沾自喜；Certicom 的股价会应声下

252

① Black Forest：德国西南部一山区，位于莱茵河与内卡河之间。为四季旅游区，以其钟表和玩具工业而著名。



跌；即使这个攻击被击退，椭圆曲线将永远无法摆脱不安全的标签。因此，西佛曼选择了一种更为学术的方法，在他即将要宣讲这个思想的会议召开之前3个星期，他将自己的设想寄给了柯布利兹。

在那个周末，柯布利兹的日程是飞往加拿大的滑铁卢，Certicom的总部所在地。Certicom的主管着急地发给他传真，希望他能够给出一个修正方案，或者说明为什么这个攻击会失败。“最初，我找不到任何原因说明西佛曼的攻击会失败。”柯布利兹习惯于在有飞行的日子早起，并且他知道自己必须做点什么来安慰在滑铁卢的朋友。当他登上飞机的时候，他突然想到如果西佛曼的攻击能成功破解椭圆曲线，那它也能同样攻破RSA。因此如果他们失败了，陪着他们的还有RSA。

“那真是可怕的一刻，”柯布利兹回忆道，“我给西佛曼发了电子邮件。在那个时候你真庆幸自己是数学家而不是商人，你开始意识到生活有时比电影还要精彩。”然而西佛曼并没有对RSA同时被牵连感到心烦意乱。他当时是一个名叫NTRU的新密码系统的开发组成员，开发组很谨慎地没有透露NTRU背后基于的理论。和其他密码系统不同，NTRU不受西佛曼攻击的影响，因此这正是NTRU公布于众的最好时机。

在两个星期之内，柯布利兹对椭圆曲线的特殊结构进行了仔细的分析，最终证明西佛曼的攻击计划在计算机上是不可行的。一种叫做高度函数的专业名词拯救了椭圆曲线，柯布利兹现在称之为“金盾”。金盾不光保证了密码系统能够抵挡西佛曼的攻击，而且还能抵挡其他方式的攻击。虽然起初有一些恐慌，但很快就恢复了平静。柯布利兹在讲座中也经常乐于讲述这段传奇，并且加上“纯数学如何搞垮电子商务”这样的标题。这个故事说明在数学世界中无论多深奥或多抽象的角落取得的进展，也有可能影响整个商业界。

这也正是为什么像AT&T和国家安全局都注视着哈代所谓的“纯洁且温和”的数论世界的原因。在20世纪80年代到90年代，AT&T实验室的负责人安德鲁·奥德兹克开始将公司的超级计算机用来探索黎曼世界中那些从未被观测过的区域。你也许会问，进行这样的计算的目的是



什么，如果不是为了找到黎曼假设的反例，那为什么花去如此多的精力和 AT&T 的经费来计算这些零点？这是因为，在听说了美国数学家休·蒙哥马利关于黎曼临界线上非常远的零点的预言之后，奥德兹克产生了兴趣。奥德兹克意识到，如果这个预言是正确的，那么这个素数故事中最奇怪也最意想不到的情节就将出现。

223

224

第十一章

从规则零点到量子混沌

发现的真实旅程并非在于寻找新世界，而在于拥有不同于别人的眼光。

——马赛尔·普若斯特（Marcel Proust），《追忆消逝的时光》（*Remeberance of Things Past*）

ζ函数世界中，位于海平面的点在黎曼临界线上是如何分布的？看起来这个问题很疯狂，但休·蒙哥马利（Hugh Montgomery）并非主动地提出了这个问题，因为大多数人认为在没有证明所有的零点都位于黎曼临界线上之前，提出这样的问题只是有勇无谋。然而，蒙哥马利在提出问题之后发现的奇妙规律为我们提供了最好的证据，告诉我们该从何处寻找黎曼假设的答案。蒙哥马利最先提出这个问题是为了帮助自己理解另一个毫不相关的、从研究生时期就开始关注的问题。蒙哥马利曾在那些看上去毫不相关的数学领域中进行过探索，试图在数学界扬名立万。突然，他就像爱丽思一样，毫无预料地跌落到了一条秘密通道中，来到一个神秘的世界，最终发现这个世界就是黎曼的虚数世界。

和一般随意穿着T恤和牛仔裤的数学家不同，蒙哥马利很注重自己的形象，他总是穿西服打领带，这样的穿着风格反映了他作为数学家的保守性格。虽然出生于美国，但蒙哥马利选择了在英国剑桥大学攻读博士学位，因为他喜欢那里优雅的学院生活。得益于20世纪60年代出现的教育革新，蒙哥马利迅速成长为一位年轻数学家。这次教育革新改变了对中学生讲授数学的方式，不同于以前将已知结果教给学生而不去解释为什么数学家可



以得到这样的结果;相反是让他们掌握数学的真正意义。蒙哥马利与其同时代人只学到一些基本的公理,更多的结果则要靠他们自己去推导。仅仅依靠推理规则,他们需要自己建造出数学的大厦,而不是像游客一样参观那些纪念碑。这一切都促使了蒙哥马利数学生涯的起步:

> 我很幸运,因为它将我带入数学世界。我在高中阶段就已明白成为数学家意味着什么。这门课程的问题在于所有的数学教师都必须接受再教育,才能够进行这门课程的讲授。我的老师恰好就是这个系统的创始人,虽然它只能针对少数的学生进行讲授,但最终的结果却是可观数量的职业数学家。

255

在高中时,蒙哥马利就喜欢探索数的性质,特别是素数。但他也发现我们对素数其实了解得很少,是否存在无穷多个孪生素数,像 17 和 19 或 1 000 037 和 1 000 039 那样?是否正如哥德巴赫所想,每个偶数都是两个素数之和?直到成为剑桥的研究生之后,蒙哥马利才听说了最著名的素数问题:黎曼假设。然而在他陷入剑桥伟大数学传统的魔法时,另一个问题吸引了他。

蒙哥马利在 20 世纪 60 年代末期到达剑桥的时候,那里正是一片欢乐气氛。数学系正为解决了伟大高斯提出的问题而进行庆祝。三一学院的成员阿兰·贝克尔(Alan Baker)在虚数分解问题上做出了重大突破。虚数分解问题是高斯在《算术探讨》中提出的问题。对于普通的数,比如说 140,它存在一组确定的素因子(这里是 2, 2, 5, 7),并且可以知道不存在另外一组素因子,它们相乘之积为 140。但是对于虚数,就没有如此好的性质,高斯惊讶地发现有时存在着多种方法,由素因子相乘得到虚数。

蒙哥马利也渴望享受到贝克尔解决高斯问题之后体验到的兴奋。他认为自己可以将贝克尔的思想推广到高斯的另外一些问题,从而在数学界成名。推广贝克尔的结论非常困难,但是蒙哥马利无所畏惧,他开始广泛地阅读,竭尽所能地深入数论研究。在剑桥,有着全世界最好的数

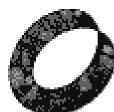


论环境，由哈代和利特伍德所强化的剑桥传统，十分适合于接受新的思想。蒙哥马利发现哈代和利特伍德曾对孪生素数出现的频率提出过一些精彩的猜想，这些猜想成为他在校期间最感兴趣的问题。

蒙哥马利同时也知道了哥德尔那令人不安的定理。在中学的时候，蒙哥马利已经知道如何在一些可接受的公理基础之上建造起数学的大厦。但根据哥德尔的理论，这样的技巧对于某些问题并不适用。因此，256 肯定会存在某些有关素数的猜想，它们不能由蒙哥马利在学校中学到的公理推导出来。如果某个打算攻克的素数问题恰好不存在证明，那该怎么办？也许蒙哥马利只是用一生的时间来追寻一个幻影。

为了拓宽自己的学识，寻求剑桥之外的思想，蒙哥马利决定去普林斯顿的高等研究院进修一年。在那里，他得到了一个机会，表达自己对不可证明性的担心。根据惯例，每个访问高等研究院的学者，无论职位如何，都会被邀请与研究院院长共进午餐。当院长询问蒙哥马利打算进行什么研究时，他说自己已经关注孪生素数猜想一段时间了，但他同时也表达了自己对哥德尔定理的困扰。院长安慰年轻的蒙哥马利说："那好，我们为什么不去问问哥德尔先生呢?"于是蒙哥马利被引见给哥德尔，咨询他的意见。但是令蒙哥马利失望的是，哥德尔也不能向他做出保证，在现有的数论公理之上，像孪生素数假设这样的问题是可以被证明的。

哥德尔曾经说过这样一段与黎曼假设有关的话：也许构成现代数学大厦基础的公理系统仍然不够广泛，不足以为黎曼假设提供证明。在这种情况之下你仍然可以继续加高数学大厦，但是一直也不会与黎曼假设发生联系。然而，哥德尔也有一些安慰的话语，他相信只要是来自于真正兴趣的猜想，一定不会遥不可及。我们需要做的就是找到某块新的基石，以此扩充数学大厦的地基。只有回到这门学科的基础之处，找到能扩充地基的东西之后，或许可以由此构造出那个消失的证明。如果这个猜想是你真正关心的——如果猜想的结果是某个已经证明结果的自然推广——那么哥德尔认为，总可以找到某块基石，它恰好可以补上地基中缺少的那部分，由此就能证明目标猜想。哥德尔曾经证明，这样的操作



只能对单个猜想有效，但是只要持续不断地进行像这样的对于数学公理基础的革命，未来将会有越来越多的未解问题得到解决。

蒙哥马利回到了剑桥，这意味着他渴望理解数字宇宙神秘性的梦想并没有完全破灭。他重新回到高斯关于分解虚数的问题，在曾经读过的资料中，蒙哥马利知道黎曼世界的特性与高斯的目标并非毫无关联，特别是在20世纪初期，黎曼假设在证明高斯某个虚数分解问题方面的矛盾境地更能说明这一点，这一问题就是所谓的高斯类数猜想（Class Number Conjecture）。

1916年，一位德国数学家埃力克·赫克（Erich Hecke）成功地证明了，如果黎曼假设正确，那么高斯类数猜想也正确。这个结论是上世纪中出现的众多条件证明之一，它们迫使我们不得不去攀登黎曼高峰，才能最终得到这些证明声称的宝藏。如果黎曼假设得不到证明，这些论述也不能被称为"证明"。数年之后，当蒙哥马利知道高斯类数猜想的另外一个结果时，他对黎曼假设似是而非的情况更加糊涂。三位数学家马克斯·都灵（Max Deuring）、路易斯·莫代尔（Louis Mordell）和汉斯·赫尔布罗恩（Hans Heilbronn）成功地证明了，如果黎曼假设错误，同样可以证明高斯关于虚数分解的猜想正确。这种情况中并没有"失败者"，因为不管怎样，总可以说明高斯关于虚数分解的直觉是正确的。结合了赫克的证明以及都灵、莫代尔和赫尔布罗恩的证明，高斯类数猜想的无条件证明是黎曼假设最奇怪的应用之一。

现在，蒙哥马利知道黎曼零点在某些高斯关于虚数分解的未解问题中的重要性。如果他能够证明零点都倾向于落在黎曼临界线上，那么就可以在推广贝克尔的结果方面获得一些进展。受到自己长期关注的孪生素数猜想的启发，蒙哥马利相信一个零点之后必然很快会出现另外一个零点。但是他能否证明这些位于海平面的点非常靠近，就像我们期望的那无穷多个孪生素数一样呢？零点的小范围汇聚会给分解虚数问题带来深刻的影响，这会不会成为蒙哥马利第一件战利品，就像众多研究生梦寐以求的、在残酷的学术界扬名立万的成果？



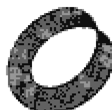
蒙哥马利压下自己的赌注，认为零点在黎曼临界线上是随机分布的，在某种意义上，这也反映了素数在数的直线上分布的表面随机性。毕竟，如果素数像看上去的那样是由抛硬币决定的话，作为公平的赌局，可以想象ζ函数的零点也应该是随机分布的。随机性总是会产生某些聚集现象，就像是三辆公共汽车同时到来，或是中奖彩票的数字经常会出现连号。蒙哥马利期望可以证明，在这种随机性的影响下，不同的零点簇非常接近。也就是说，在他向着临界线北部进发时，蒙哥马利能看到一连串的零点簇，这样就可以证明虚数分解中的某些问题。

258

问题在于，目前只有相当少的证据。只有少数的零点被计算出位置，这样的条件根本不可能直接看出零点的汇聚，因此蒙哥马利需要采取另外的方法。由于缺少实验证据，是不是存在某些理论预言了这样的汇聚情况呢？蒙哥马利所做的就是将通常零点的角色进行一次有趣的逆转。黎曼利用ζ函数发现的公式表达了素数和零点之间的直接联系，推广这个公式后，就可以利用对零点的探索来理解素数。而蒙哥马利所做的是将这个公式反过来写，这样他就可以利用素数的知识来推导出黎曼临界线上零点的行为。蒙哥马利记得哈代和利特伍德曾猜测孪生素数出现的频率，也许他可以将这个猜想推广到零点行为上。但是当他将哈代和利特伍德的猜想运用到黎曼公式上时，出乎他的意料，公式预言零点根本不会产生汇聚的现象。

蒙哥马利开始进一步探索这个预测的细节。看上去整个预测是说，当某人沿着黎曼的临界线向北方探索时，零点——和素数不同——互相之间存在着排斥作用。蒙哥马利迅速意识到零点根本不可能产生汇聚的现象。和素数的行为不同，零点后面不会伴随着另外的零点。实际上，蒙哥马利的预测提示我们，零点也许在黎曼临界线上以完全一致的方式有序的排列，而不是像他原来期望的那样具有随机性（参见图38）。

蒙哥马利寻找一种方法，来描述自己关于这些位于海平面的点的间隔的大小。他准备用所谓的成对关系图来表示零点之间间隔的大小（参见图39）。最终结果与蒙哥马利见过的所有图像都不同。如果你随机选



择一组人群，并用图形描述出他们身高的差距，那么你会得到经典的高斯钟状曲线①，但是蒙哥马利的图形与此完全不同。

蒙哥马利图形记录了对于每个可能的间隔距离究竟有多少对零点满足条件。最初的图形表示零点不希望靠得太近，因为图形的高度一直很低。蒙哥马利相信，图形的右方将会出现波动的图形，体现出在统计学中不同寻常、特殊的情况。蒙哥马利无法证明这确实就表示了零点之间的距离，同时也没有足够的零点位置的计算结果来验证这个预言的正确性。这个奇怪图形的方案只是单纯地基于哈代和利特伍德关于孪生素数出现频率的猜想。因此，这个图形也不像蒙哥马利原先所想的那样具有创新性。 259

由于蒙哥马利最初期望的是发现零点的汇聚现象，因此他认为自己的工作在某种意义上应该算是失败。他还曾经计划利用零点在临界线上的汇聚来解决高斯关于虚数分解的未解问题，结果事与愿违。如果蒙哥马利的新猜想正确，零点确实是互相排斥的，那么他原先的思想就没有什么意义。事实上，当你开始进行探索的时候，你根本无法知道终点在哪里。在剑桥的时候，利特伍德曾建议蒙哥马利，“不要害怕从事难题的研究，也许在这个过程中你会得到某些有趣的结果。”这个名言是利特伍德在艰苦的研究生阶段学到的，当时他的导师随意地交给他解决黎曼假设的任务。 260

蒙哥马利于1971年无意中发现了这个意料之外的零点间距分布图。到了1972年3月，他完成自己的博士答辩并接受了密执根大学的职位，现在他已经是那里的教授。蒙哥马利相信自己的观点是全新并且有趣的，但是他仍然心存疑惑。当时的塞尔伯格相当于过去的高斯，“塞尔伯格有许多未发表的论文，总是会担心他说出，‘啊，是啊，这个结果我早知道了。’”就像是勒让德宣称的新发现最终被证实是高斯在数年前就记录在未发表的手稿之中的旧结果，而现在，数学家经常发现自己被塞尔伯格击败。由于在与厄多斯合作给出素数定理的初等证明过程中受 261

---

① 这里指的是统计学中正态分布曲线。





图 38　随机雨滴、素数和黎曼零点之间的间隔

到的伤害，塞尔伯格坚持独自一人在数论中探索，其中许多结果都没有发表。

因此，在蒙哥马利出发参加 1972 年春季的一场数论会议时，他顺道访问了普林斯顿，将自己的结果告诉塞尔伯格。但是还有其他的事困扰着他："我有点困惑，因为我所做的一切应该有一个解释，但是我不知道这个解释是什么。"然而最后帮助蒙哥马利获得解释的人并不是塞尔伯格，而是另外一位普林斯顿帮的成员。



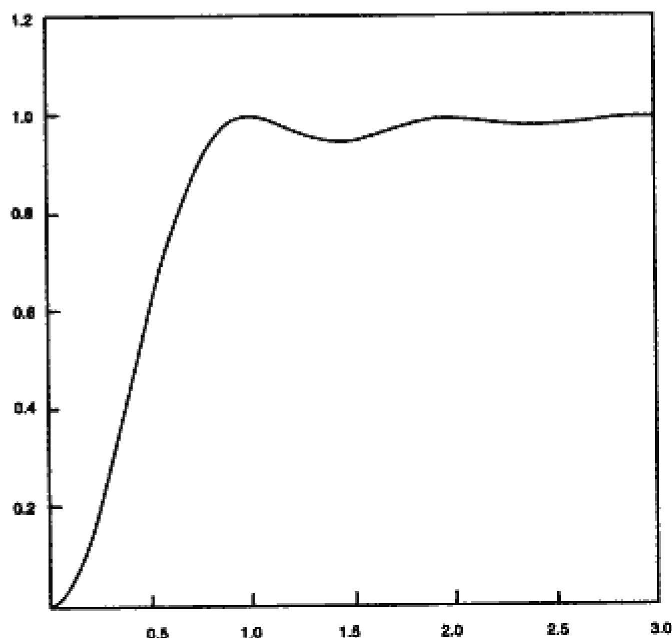


图39 蒙哥马利图形：横轴表示每对零点之间的距离，竖轴表示对于给定距离有多少对零点

戴森，物理学的青蛙王子

英国物理学家弗里曼·戴森（Freeman Dyson）早在战后就因为支持独行科学家理查德·费曼（Richard Feynman）而声名大噪。在得到剑桥的学位之后，戴森获得了在康奈尔大学进行物理研究的奖学金。正是在那里，戴森碰到了年轻的费曼，费曼正试图将非常独特的个性带入到量子物理中。起初，许多人都无视费曼的观点，因为他们无法理解费曼那非常有个性的语言。戴森则对费曼提出的观点非常欣赏，并帮助他清晰地表达出自己革命性的思想。费曼发明的工具现在是粒子物理中绝大部分计算的关键，如果没有戴森的阐释能力，这些工具也许根本不会



出现。

最初引发戴森想象力的并不是物理学。他出生于一个有着深厚音乐传统的家庭，对科学并没有什么兴趣。然而在学校中，数学的旋律深深地吸引了年轻的戴森。在赢得了一本哈代的书籍后，他开始着迷于拉马努扬的分划数，“从那天之后的40年里，我时常回到拉马努扬的花园中漫步。当我回到那里的时候，我发现那里盛开着新鲜的花儿。这是拉马努扬最杰出的成就，他发现了许多结果，同时也在花园中留给后人许多等待发现的结果。”

用戴森的语言，虽然科学家在同一领域中探索，但是他们却分成两派：鸟类和蛙类。鸟类高飞在该领域的上空，可以看到地面上大量的关系；而蛙类则在自己非常熟悉的小池塘中游泳或在泥泞中跋涉。数学是非常适合于鸟类科学家的领域，而戴森认为自己是一只青蛙，循规蹈矩地在物理实际问题中探索。

262

由于戴森成功地宣传了费曼的量子物理学，曾经在二战期间领导美国原子弹计划、现在是高等研究院的负责人罗伯特·奥本海默（Robert Oppenheimer）注意到了他，1953年戴森接受了奥本海默提供的研究院的终身职位。虽然戴森的性格比较谦逊、不善言语，但是他直爽的性格为他在学术圈之外也赢得了好名声。戴森还因为相信地外文明的存在而知名，在痴迷于外太空的大众心中，他被疯狂地崇拜。因为在20世纪50年代末和60年代初期他曾领导一个叫做俄里翁计划①的工作，这项计划打算建造飞向火星和土星的载人航天器。

虽然蒙哥马利于1970至1971年期间在高等研究院进行过访问，在那里他曾初次见到哥德尔，但是他与物理学家之间并无太多联系。在普林斯顿他根本没有闲暇与众多数论学家之外的人谈话，但是他回忆说，“我曾看见过戴森，虽然我怀疑他是否知道我是谁，但我们还是互相微

---

① Orion Project，俄里翁是希腊神话中一个巨人般的猎人，普勒阿德斯的追求者、厄俄斯的恋人，被阿特密斯所杀。天文学中用来命名猎户座。



笑点头示意。我知道他是因为他曾经在“二战”期间的伦敦进行过数论研究。”

在会前的顺访中，蒙哥马利在普林斯顿向塞尔伯格以及另外几位访问高等研究院的数论学家解释了自己的思想。讲了一段时间后，他们开始休息，进行一项在大部分数学系中已成惯例的活动——下午茶。茶点时间在研究院是非常重要的活动，因为来自不同领域的学者可以借此交换彼此的想法。与蒙哥马利交谈的是参加报告的一位数论学家萨拉瓦达姆·周拉（Saravadam Chowla），周拉是利特伍德的印度学生。在1947年印度和巴基斯坦建国时，周拉的家乡拉合尔（Lahore）成为了巴基斯坦的一部分，因此他逃到了美国。周拉是研究院的定期访问者，因为活泼而且幽默的性格得到众人的喜欢，他最后成为了研究院的终身成员。当周拉和蒙哥马利交谈的时候，这位印度的数学家发现了偶然经过的戴森。

“周拉说，‘你见过戴森吗?’我说没有。‘那我来为你们介绍’，我说不用了。”但是周拉向来不允许别人说“不”——他是唯一能够威逼塞尔伯格写出合作论文的人。“周拉坚持要为我介绍，并把我拽过去开始介绍。我对打扰戴森感到很不好意思，但是戴森很热情，他问我最近在干什么。”于是蒙哥马利开始谈论自己的想法，关于零点对之间间距可能有的行为。当蒙哥马利提到自己关于间距的分布图时，戴森的眼睛发出了光芒。“这不正好就是随机厄米特矩阵特征值对之间间距的行为吗!”

263

随后戴森向蒙哥马利解释，这个听上去很奇怪的数学概念早已被量子物理学家用来预测当一个重原子被低能量中子轰击时原子核的能级变化。作为这一领域的前线人物，戴森告诉蒙哥马利几个已经做过并且记录了能级的实验。毫无疑问，当蒙哥马利查看铒（元素周期表中第68位的元素）原子核的能级之间的间距时，他发现了惊人的相似性。如果他从黎曼临界线上取出一串零点，将它们与实验记录的能级并排放在一起，立刻就可以看出两者表现出神秘的相似。无论是零点还是能级都强



烈的倾向于有序模式而非随机选择。

蒙哥马利对此几乎不敢相信。自己预测的零点分布模式居然就是量子物理学家在重原子核能级中发现的模式。这两种模式是如此的特殊，以至于这种强烈的相似性不可能是巧合。这就是蒙哥马利在寻找的预言：也许重原子核中量子能级背后的数学就是决定黎曼零点位置的数学。

用来解释这些能级的数学可以追溯到激发 20 世纪量子物理学革命的那个新发现。像电子和光子这样的基本粒子拥有两种看上去很矛盾的特性，某一方面它们的行为可以看作是微小的弹子球，然而实验也表明只有把这些基本“粒子”看作波才能解释另外的特性。量子物理的产生就是试图解释这种亚原子世界中的双重人格——波粒二象性。

量子鼓

在 20 世纪初期出现了原子图像，它像一个微小的太阳系，其中包含着那些不可分的粒子。位于这个迷你太阳系中心的“太阳”被称为原子核，后来物理学家发现原子核是由叫做质子和中子的粒子构成。围绕着原子核转动的是电子，就像是原子结构中的行星。但是理论和实验的进步促使物理学家重新思考这个模型，他们开始认识到原子的行为与行星系统并无太多相似之处，而更像一个鼓。当你敲击鼓的时候，产生的振动是由某些具有固定频率的基本波形构成。理论上存在着无穷多种可能的频率，因此鼓声应该是这些不同频率的组合。与小提琴弦的和弦不同，鼓发出的声音是由鼓的形状、鼓皮的张力、外部空气的压力以及其他因素决定的频率的复杂组合。鼓产生的不同波形的复杂性解释了为什么在管弦乐队中打击乐器为什么无法发出一个可辨认的音符。

264

有一种方法可以让我们看到构成鼓声的振动的复杂性。18 世纪的科学家厄斯特·克拉德尼（Ernst Chladni）发明了一个实验，并在欧洲的宫廷中进行表演。（拿破仑对他的表演特别着迷，并因此奖赏给他



6000法郎。）克拉德尼用一个方形的铁盘代表鼓，当他敲击铁盘时，铁盘会发出巨大的响声。但是利用小提琴弓摩擦铁盘，克拉德尼可以巧妙地挑出铁盘不同的频率。在铁盘上铺上一层细沙，克拉德尼就可以展现给观众铁盘振动时的每个基本频率的不同形状。当铁盘停止振动时，沙子会汇聚到一起，呈现出奇怪的图像。每次克拉德尼利用琴弓使铁盘振动时，细沙就会构成一个新的图形，表示这是一个新的频率（图40）。

物理学家在20世纪20年代认识到，用来描述鼓声频率的数学同样可以用来预测电子如何在原子中振动的能级。原子中的限制对应于鼓的外界因素：原子中的作用力控制着亚原子粒子的振动，如同鼓皮的张力或外界气压控制着鼓的振动，从而决定发出的声音。每个原子都像克拉德尼的铁盘，原子中的电子只能以某些固定的模式振动，就像克拉德尼展现的图像一样。如果我们改变电子的能量，它就会以一个新的频率振动，与此相似，克拉德尼利用小提琴弓可以让铁盘中的沙子呈现出不同的图像。周期表中不同元素的原子都有自身独特的频率组，电子总倾向于以这些频率振动。这些频率是原子独有的身份信息，可以被光谱学家用来从本质上辨别观测对象的原子种类。 265

为了研究鼓表面出现的振动模式（或称为波形），人们发展出一套数学理论。这套理论可以追溯到欧拉的波方程，将鼓的一些物理属性——形状、鼓皮的张力、外部气压等等——代入方程中，其结果就是可能出现的波形。原子物理与鼓的物理很不相同，因为它涉及虚数，也正是虚数赋予量子物理奇怪的概率特性。

在我们日常生活的宏观世界中，我们可以对物体进行测量而不影响它本身。当我们用秒表为运动员测量时间时，我们不会影响他们的速度；当我们测量标枪的落点时，我们不会搞错投掷的距离。作为观测者，我们独立于被测量的系统。但是在微观世界中，事情就变得不一样。当我们观测一个电子时，我们和它有相互作用，不可避免地会影响它的行为。 266

量子物理试图解释在观测者介入之前粒子的行为。在无法被我们从

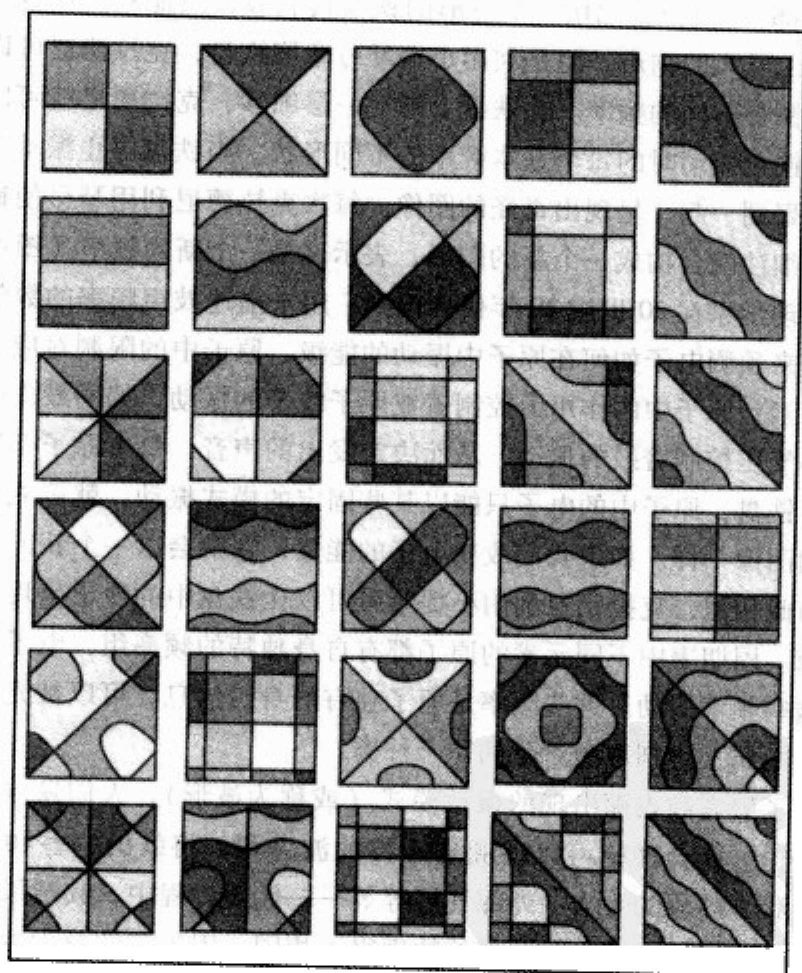


图 40　克拉德尼用来取悦拿破仑的铁盘的部分奇怪振动图像

宏观世界中观测到的很长时间中，量子世界仅仅存在于虚数世界中。正是这些虚数解释了那些看上去无法以我们宏观世界角度解释的观测结果。比如说，一个电子在观测之前可能同时位于两个不同的位置，或者以不同的频率或能级振动。当我们在量子世界中观测一个现象时，似乎我们看到的并不是现象自身的范围，而是这些现象投射到我们“真实”实数世界中的映像。观测本身会导致二维的虚数世界坍缩为一维的普通



实数直线。在我们观测电子之前，它可能会像鼓一样，以多种频率的组合进行振动；但是当我们观测它时，我们不可能像听到鼓声那样听到所有的频率同时出现，我们听见的只是电子在某一单一频率的振动。

为我们描绘量子世界图像的两位重要人物是哥廷根的物理学家沃纳·海森堡（Werner Heisenberg）和马克斯·波恩（Max Born）。希尔伯特经常从自己的窗户中看见楼下数学系外的草坪上，海森堡和波恩两人来回走动，激烈讨论20世纪以来的原子模型理论。海森堡发展了一套振动的数学来解释原子中的能级，希尔伯特曾设想过是否黎曼世界中的零点位置也可以用它来解释，但是当时并没有进一步地进行研究。蒙哥马利的发现重新复苏了希尔伯特的思想，理解黎曼零点的最好方法也许来自波恩和海森堡创立的用来解释能级的量子鼓的数学。虚数和波的混合带给量子鼓一组特殊的特征频率集合，这一理论来源于量子物理而非古典管弦乐队。但是当蒙哥马利在普林斯顿的休息室中从戴森那里听说这些时，与黎曼零点位置最相符的特征频率却是来自量子管弦乐队中最复杂的原子。

267

迷人的旋律

量子物理学家最先分析的原子是氢原子。氢原子是最简单的鼓：只有一个电子围绕着一个质子转动。决定这个电子和质子的频率或能级的方程非常简单，因此可以被准确地解出。这个电子的频率与小提琴弦产生的和弦有很多相似之处。虽然量子物理学家成功地解决了氢原子，但是当他们进一步研究周期表中的原子时，他们发现用数学准确地描述这些量子鼓是一件不可能的任务。原子核中含有的中子和质子越多，围绕它们转动的电子越多，任务就会变得越艰巨。当他们处理含有92个质子和146个中子的铀238的原子核时，物理学家就完全不知所措了。最困难的问题是决定原子系统中处于中心地位的原子核的可能的能级，首先计算出决定原子核能级的数学鼓的形状就是一项非常复杂的工作，其



次即使物理学家可以找出决定这些能级的数学鼓，那么也会因为鼓太复杂而无法决定它们的频率。

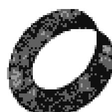
直到19世纪50年代，人们才找到一种方法来分析这些复杂的结构。并非试图找出这些不同能级的具体数值，尤金·魏格纳（Eugene Wigner）和列夫·朗道（Lev Landau）决定研究这些能级的统计量，他们关于能级的工作利用了高斯处理素数的思想。高斯曾经放弃试图精确预测每个素数何时出现的工作，而转到估计当我们考虑更多数时平均会出现多少个素数这样的问题。以同样的方法，魏格纳和朗道提出了一种更易操作的方法来理解原子的能级。这个统计方法可以揭示在所有频谱的一小段区域中发现原子核能级的可能性。

铀的原子核非常复杂，对于铀的不同状态，有许多可能的方程来决定它的能级。因此如果随着原子核的状态不同，这些能级的统计量也产生显著的变化，那么获得这些统计量的可能性就微乎其微。由于能级可以通过分析量子鼓来决定，魏格纳和朗道决定看看在改变鼓的形状时，这些频率的统计量是否产生巨大的变化。幸运的是，对于大多数的量子鼓，这种情况不可能发生。魏格纳和朗道发现，当他们随机地改变量子鼓时，也许特定的频率会产生变化，但是频率的统计量却不会产生变化。虽然大多数量子鼓的统计量都相同，但是这是否意味着重原子原子核的运动就和平均量子鼓一样？魏格纳和朗道相信描述铀元素原子核的量子鼓并无任何特殊之处，也就是说，它们与大多数量子鼓基本相同。

268

魏格纳和朗道的猜测最终被证实。当他们将随机量子鼓的能级统计量和实验中观测到的能级统计量相对比时，它们十分吻合。特别的是，当他们观察铀原子核中两个能级之间的距离时，看起来能级之间是互相排斥的。这也正是弗里曼·戴森在普林斯顿与蒙哥马利交谈时显得如此兴奋的原因——蒙哥马利展现给他的那幅图像正显现出能级的特征图形。但是蒙哥马利却是在一个看上去与科学无关的领域发现了这一图像。

随后的一个问题就是，为什么这两个领域——能级和黎曼零点——



彼此之间会产生联系，它们如何产生联系。蒙哥马利肯定像考古学家在世界两极的洞穴中发现旧石器时代壁画一样感到不可思议，但是两者之间必然会存在某种联系。蒙哥马利承认与戴森的谈话肯定是科学史上最幸运的事情，“这真是奇遇，我恰好出现在正确的地方。”自从伽利略和牛顿时代以来，物理和数学经常会涉及相似的领域，但是谁也没有预料到黎曼数论和量子物理会有如此密切的联系。蒙哥马利试图理解分解虚数的努力没有任何结果，但是他却偶然发现了更有意义的结果。“比起失败的原计划，这个结果比所有的都要好，”蒙哥马利笑着说。

这个在普林斯顿茶点时间的新发现对黎曼假设意味着什么？如果黎曼世界中位于海平面的点可以用物理学中描述能级的数学来解释，那么就有一个令人兴奋的机会来证明为什么所有海平面上的点都落在同一条直线上。某个零点落在临界线之外就像存在着一个虚数能级，量子物理中的方程告诉我们这一点绝不可能发生。这是提供某种关于黎曼假设的解释的最好希望。

虽然实验已经证实了魏格纳和朗道关于大质量原子的能级模型，蒙哥马利仍然没有得到任何的实验结果，可以证实黎曼世界中位于海平面的点具有像他相信的理论所预测的那样的行为。没有人进行过实验，来观察这些零点是否像他预测的那样真的互相排斥。因为真正的困难在于，这些统计结果最有可能出现的位于黎曼世界中的区域，远远超出当时蒙哥马利的计算能力范围。

269

在剑桥，蒙哥马利已经从利特伍德的结果中了解到，必须在素数序列上走多远才能了解素数的真正本色。尽管利特伍德已经在理论上证明了高斯关于素数个数的猜测将在某处变为过低估计，但是没有人能成功地在实验中证实这一点。蒙哥马利不可避免地也要承受这个命运。对实验物理学家而言，需要足够长的时间才能建造出能产生足够能量的粒子加速器来证实魏格纳和朗道的预测。蒙哥马利害怕数学家永远无法计算到足够大的数，来验证是否临界线上足够远的零点的行为都像他预测的那样。



但是蒙哥马利没有考虑到在新泽西州核心地带 AT&T 实验室的安德鲁·奥德兹克和他的克瑞超级计算机的计算能力。当奥德兹克听说了蒙哥马利关于零点对之间间距的预测，以及与之平行的重原子核能级背后的随机量子鼓的结果之后，他觉得这正是他所期望的挑战。奥德兹克开始计算黎曼临界线上直至 10^{12} 单位远的零点，这是计算史上非常杰出的成就。如果我们想象黎曼世界的地图是以新泽西为中心，黎曼临界线上每个单位长度看作 1 厘米，那么奥德兹克计算的黎曼临界线的最远区域将是地球与月球距离的 25 倍。只要克瑞超级计算机算出 10 万个零点，奥德兹克就可以计算它们之间间距的统计量。到了 20 世纪 80 年代中期，奥德兹克发表了自己的计算结果，黎曼世界中的零点确实与重原子能级之间的间距表现出了某种相似性，但是也清楚地显示出它们并非完全吻合，这样的结果是统计学家不能接受的。是蒙哥马利错了，还是他需要研究更远的零点？

奥德兹克并不满足于原先任务的范围，他决定考虑 10^{20} 单位之内的零点。用我们刚才以新泽西为中心的虚拟地图来描述，奥德兹克现在探索的范围远达 100 光年，这样的距离比卡尔·萨根《接触》中发出素数信息的织女星①还要远。在 1989 年，奥德兹克将如此距离之内的零点间距标识出来，并与蒙哥马利的预测相对比。这一次的对比结果出乎大家的意料，零点的新观点终于有了令人信服的证据。在远达 10^{20} 这样的距离上，素数终于发出了明确的信息，表明它们是由某些复杂的数学鼓产生。

270

数学魔术

安德鲁·奥德兹克发现的统计学上的吻合究竟有何伟大之处？也许像这样的统计结果可以由完全不相关的数学得到。蒙哥马利和奥德兹克

① 织女星，英文名 Vega，天琴座中的一颗亮星，距离地球大约 27 光年。



是否为我们指出了正确的方向，还是把我们引向一条白费力气的歧途？

对于这些问题的答案，我们只好去询问斯坦福统计学家普尔斯·迪亚科纳（Persi Diaconis），他是揭露通灵现象的大师，并且他还揭穿了那位宣称解决“圣经密码”——在古希伯来文献中的隐藏信息——的人的真面目。在看到了黎曼函数的数据之后，迪亚科纳承认很难找到更好的统计学上的匹配。“我从事了一辈子统计学，从没有见过如此吻合的数据。”迪亚科纳比其他人都更清楚，从一个角度看上去很好，就需要从其他所有的角度来检查，以保证某些明显的缺陷不会被忽视。迪亚科纳是这种把戏的大师——最初吸引他想象力的是魔术，而非数学。

在纽约度过童年的迪亚科纳，整日逃学游荡在魔法店中。他熟练的技巧曾引起一位美国大魔术师戴·维尔农（Dai Vernon）的注意。迪亚科纳回忆说，当时68岁的维尔农，希望他能够作为助手加入自己的巡回演出：“我明天要去特拉华州，你想和我一起去吗？”14岁的迪亚科纳瞒着父母，收拾行装就出发了。在接下来的两年里，他们周游了全国：

> 我们就像奥利弗·退斯特和法更①。魔术团体是有着广泛支持的团体，它并不是低俗的表演团体，或者像那样的团体，它是中上层阶级魔法爱好者的团体。魔术师对赌徒很有兴趣，维尔农和我经常会找出那些要花招的赌徒。如果我们听说某个爱斯基摩人可以用雪地鞋发出第二张牌，我们就会立刻去阿拉斯加——这就是我们的冒险。我们在那两年中一直做这件事，只需跟着消息走就可以。在与这些赌徒打交道的过程中，总是要谈到几率问题，因此我开始对概率论感兴趣，并希望进一步了解它。

271

在旅途中，迪亚科纳开始阅读关于概率论的数学书籍。也许是命运的安排，一本特别的教材触发了我们当代最有魅力的数学家的学术生

① 这两个角色都是出自英国作家狄更斯的名著《雾都孤儿》。



涯。迪亚科纳得到了威廉·费勒（William Feller）的概率论书籍《概率理论及其应用》（*An Introduction to Probability Theory and Its Application*），这是大学中该学科的标准教材之一。由于没有微积分基础，迪亚科纳完全无法读懂这本书。他知道想要前进的唯一方法就是参加纽约城市学院的夜校。困难一点点地被解决，在不到两年半的时间中他顺利毕业，并且渴望申请研究生阶段的学习。哈佛大学给这位不同寻常的学生敞开了一扇大门。

迪亚科纳仍然对自己的魔术根源有深厚感情，他承认两种艺术之间有着许多共同点：

> 我做数学的方法与魔术很相似。在这两个领域中，你总是试图去解决一个有着各种限制的问题。在数学中，这个限制表现在你必须使用手头拥有的工具给出合理的论断；在魔术中，你必须利用工具和熟练的手法来表现一个效果，而不让观众察觉到你在做什么。在这两个领域中解决问题的智力过程也基本上相同，唯一存在于魔术和数学之间的差别是竞争。数学中的竞争比魔术领域要厉害得多。

作为一位统计学家，迪亚科纳对某件事是否随机很感兴趣，他还因为关于分析洗牌的工作而上了《纽约时报》的头版。根据迪亚科纳的理论，对一位公平的牌手而言，他需要进行7次洗牌才能得到一副随机排列的牌，但这是在公平牌手和公平洗牌条件下的结果。但如果洗牌的人拥有像迪亚科纳那样的魔术之手，情况就会大大不同。很多魔术都依赖于迪亚科纳实施完美洗牌的技术，因为他知道通过8次完美洗牌之后，牌的顺序会与原先的顺序相同，而观众则会认为牌的顺序是随机的。迪亚科纳还非常关心洗过的牌是否处于某种“做手脚”的状态，这是迪亚科纳自己取的名字，用来检测牌中是否存在某种规律，而这样的牌型在外人看来是完全随机的。他的这项工作是受拉斯维加斯的聘请，检测电子洗牌机是否为眼尖的赌客提供了类似这样的规律。

当数论学者开始传播蒙哥马利和奥德兹克的结果，黎曼世界中的零



点看上去很像某种随机鼓的频率的时候，迪亚科纳也产生了特别的兴趣。如果说有人适合找出其中的关键，那肯定就是他。“于是我打电话给奥德兹克，说我需要一些零点的数据。于是他给了我大约从 10^{20} 开始的 5 万个零点数据。”然后迪亚科纳开始用自己在 AT&T 担任电话加密工作时发明的方法来进行测试。“我进行了彻底的测试，发现它们与预测的结果完全一致，”迪亚科纳说。这是更进一步的证据，说明零点确实来自一个随机数学鼓的敲击，而这个鼓的频率和量子物理中能级的行为相似。对迪亚科纳而言，素数和能级之间的联系并非是大自然恶意的欺骗，而是真正的魔术。

272

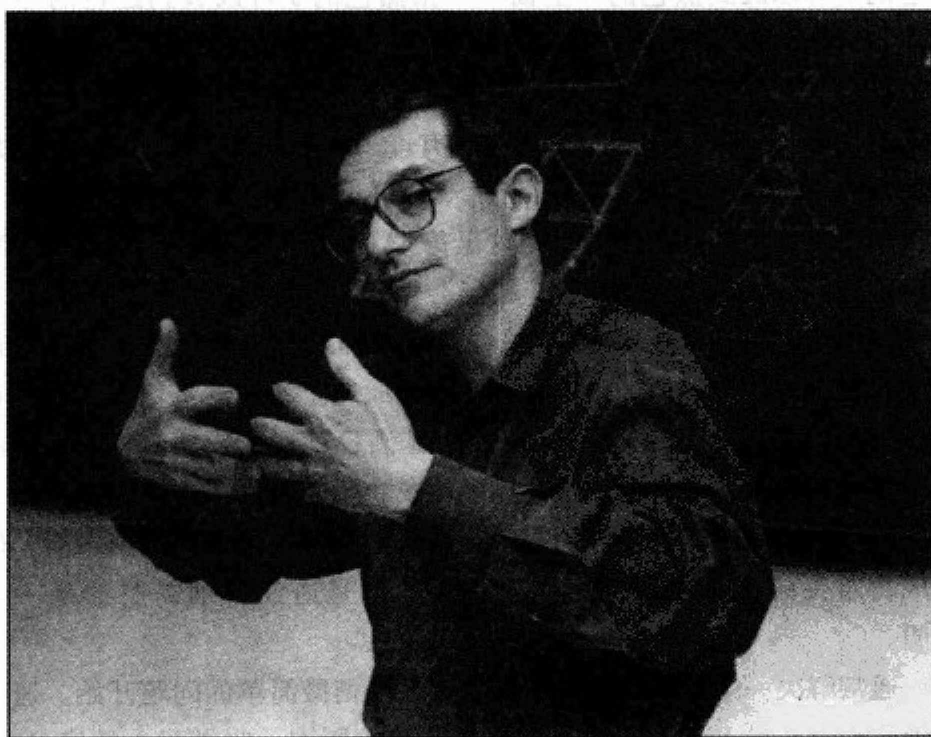
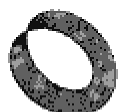


图 41　普尔斯·迪亚科纳，斯坦福大学教授



一旦这些新的统计量被发现，它们就会在每一个地方显现：重元素的原子核、黎曼 ζ 函数的零点、DNA 序列、玻璃的性质。最奇怪的是，迪亚科纳发现这些统计量也许能帮助解决另一个未解问题：期望赢得耐心游戏（game of patience）的频率。

在最常见的一种耐心游戏中，有 7 堆纸牌，第 1 堆中有 1 张纸牌，第 2 堆中有 2 张纸牌……一直到第 7 堆中有 7 张纸牌。每一堆纸牌最上面一张是翻开面朝上的，多余的那些纸牌则 3 张 1 组面朝下放置在桌面的左上方。允许的移动是，将一张翻开的纸牌移动到另一张翻开的纸牌上面，如果两张牌的颜色不同并且前者恰好比后者小 1。比如说，一张红色的 7 可以放到黑色的 8 上面，一张黑色的 J 可以放到红色的 Q 上面。当 A 出现的时候，它被放到固定位置，并且在它之上可以按顺序放置同花色的纸牌直至游戏结束。这个游戏有许多名称，包括 Klondike 和傻子的快乐（Idiot's Delight），同样也有许多该游戏的变种。在拉斯维加斯，你可以花 52 美元开始一局新游戏，只不过你不能连续不断地翻开左上角 3 张 1 组的剩余纸牌，在这里每张牌你只能看一次，而每当你移动 1 张牌到规定的固定位置时，赌场会付给你 5 美元。

273

即使这个游戏早在 1780 年左右就有人开始玩，并且被几乎每一位个人计算机的用户熟知，也没有人知道完成这个游戏的平均成功率。在拉斯维加斯一张牌就值 5 美元，因此知道自己面对的成功概率应该是值得一做的事。当迪亚科纳试图计算平均成功率的时候，这样一个看上去如此简单的游戏居然也足够的复杂。从他这么多年搜集的数据来看，似乎成功通关的概率在百分之十五左右，但是迪亚科纳需要的是一个证明。

通常解决一个数学问题的策略是从一个稍微简单的问题开始。迪亚科纳已经分析过 Klondike 的一个比较简单的版本，叫做耐心排序（patience sorting）问题。他激动地发现赢得这样一个简单耐心游戏的频率，其核心恰好位于那些数学鼓频率的理论之中。除了自己的进展，他相信要获得 Klondike 的完整分析结果还需要我们进行长期的研究。他向自己

274



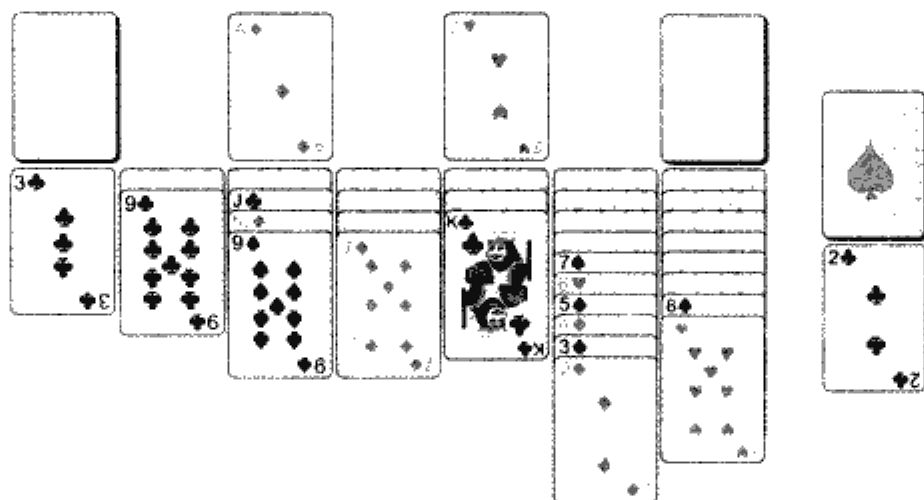


图 42 Klondike 或傻子的快乐，最流行的耐心游戏之一，数学家无法解决的谜。

的学生保证，如果谁能够作出突破，一定可以登上《纽约时报》的头版。抛开它们与随机数学鼓的微妙联系，Klondike 和黎曼假设问题的答案依然在我们的能力之外。

量子台球

数论学家试图去理解自从蒙哥马利和戴森喝了一杯茶之后给自己学科带来的奇怪转折。虽然蒙哥马利的分析看上去意味着是量子鼓的物理行为决定了黎曼零点，但是并没有太多的结果支持这一新理论。这个奇怪的鼓藏在哪里？从目前已知的统计量和证据来看，这个鼓和其他随机选择的鼓没有什么不同，因此这些数据对于找出这个决定黎曼零点的特殊鼓并没有太多帮助。当这个奇怪的联系被进一步研究之后，可以看出这个与量子物理的联系并非黎曼零点故事中唯一奇怪的事情。在数学家搜寻鼓的道路中出现了一个新的关系。

迪亚科纳和其他统计学家已经发明了一系列复杂的武器来检验给定



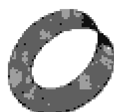
的任何命题。圣经密码以统计学观点来看是非常有意义的，因为它的支持者总是只让你从某一角度来看这些数据。正是在其他检验的压力之下，圣经密码最终被推翻。虽然迪亚科纳的研究并没有推翻蒙哥马利的预测，但是在新泽西的奥德兹克还是有点怀疑自己的计算结果，于是他开始使用一种新的统计方法来检测在黎曼零点和量子物理之间的联系是否真正存在。随后他注意到在黎曼零点的数据中出现了一些令人困扰的矛盾。

奥德兹克考虑的是一个称为数差（number variance）的统计量图像。首先他作出对应于黎曼零点的图像，然后与对应于随机量子鼓产生的频率的图像相对比。当他观察这些图像如何变化的时候，尽管刚开始两幅图像很吻合，但是黎曼零点的图像会突然偏离随机量子鼓的预测图像。图像的开始部分仍然考虑的是相邻零点之间的距离，但是当奥德兹克分析图像的连续变化时，他发现矛盾开始出现。随着图像的延伸，它描述的已经不再像初始部分那样是相邻零点间距的统计量，而更像是描述类似于第 N 个零点和第（$N+1000$）个零点之间距离的统计量。奥德兹克起初觉得是自己犯了计算错误而导致这种偏差，后来的事实证明，奥德兹克目睹的正是20世纪科学的另一个主旋律影响黎曼世界的第一个证据，这个旋律的名字叫做：混沌理论。

275

和量子物理一样，混沌理论也正逐渐融入大众文化的主流之中。20世纪90年代的锐舞派对中总少不了投射在墙上的分形图案。抛开表面的复杂性，分形其实是由非常简单的规则生成。而在这些图案背后的数学——混沌理论——可以解释为什么在简单的规则之下，生成的实体却是如此复杂。“混沌”一词最初用在动力系统中，表示一个系统对于初值非常敏感，即使实验的初始阶段做了极微小的改变，最后的结果也将出现戏剧性的偏差，这正是混沌的特征。

混沌数学的一个具体表现是台球游戏。如果你在台球桌上击打一颗球，它运行的路径是由这颗球与桌边绒布碰撞的角度决定。有趣的是，如果你在击球的时候稍微偏一点点角度，那么它的路径与前一次相比会



产生巨大偏差吗？这个答案依赖于球桌的形状。在通常的长方形球桌上，球的路径不会产生混沌行为（只有最业余的选手才会那么想）。此时的路径是可预测的，击球的初始方向发生微小的改变也不会对球的路径造成很大的影响。然而，如果在一个类似于体育场形状的球桌上，球的路径则具有完全不同的特征。如果现在我们以极微小的方向偏差击打两颗球，我们会发现它们会沿着看上去毫不相干的两条不同路径滚动（图 43）。体育场形状球桌中的物理是混沌的，而不是长方形球桌中完全可预测的路径。

当混沌数学在 20 世纪 70 年代出现的时候，许多量子物理学家对这个新理论对自己学科的影响很感兴趣。特别的是，他们想知道如果在原子大小的范围内进行这样的台球游戏，会出现什么结果。因为从某个角度看来，电子的行为就像是微观的台球。

利用现在用来制造电脑芯片的半导体材料，可以在针尖大小的范围内制造出数百个微小的台球桌，从而使得物理学家可以研究电子在如此小的台球桌上的碰撞运动。此时电子不再被限制在原子中，它可以在半导体中自由地运动，这也正是电脑芯片中传输数据的技术。此时电子的路径并非毫无限制，虽然它不再需要围绕原子的原子核转动，但是它受到球桌边界的限制。物理学家感兴趣的是，在不同形状的球桌中，是什么影响着电子的波动行为，同时还影响着电子的粒子行为——像台球那样的运动。就像被限制在原子中的电子只能以特定的特征频率振动一样，一个自由电子在微小台球桌上运动时也只能以特定的频率振动。

276

当物理学家分析能级的统计量时，他们发现随着球桌引起混沌路径和规则路径的不同，对应的统计量也不一样。如果电子被限制在一个长方形区域内运动，描绘出规律的、非混沌的路径，那么它们的能级是随机分布的。特别之处在于，这些能级常常聚集在一起。然而，如果电子被限制在类似于体育场的区域中运动，它的路径将会是混沌的，同时这些统计量会出现很大的差异。此时能级不再是随机出现，而是以一个更加一致的模式调整自身，并且任何两个能级都不再靠近。

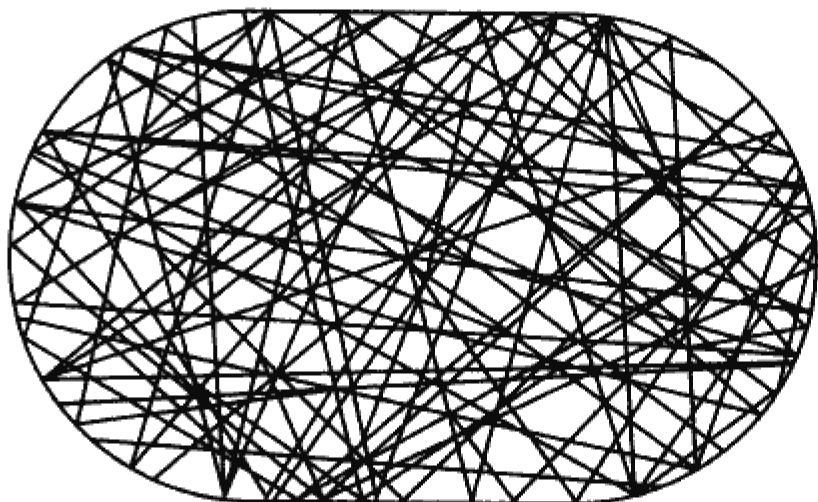


图 43 混沌运动：图中路径表示台球在类似于体育场的台球桌上的运动

277

这是另一个表现能级间奇异的互相排斥现象的例子。在混沌量子台球实验中观察到的规律，已经在重原子的能级以及蒙哥马利和奥德兹克在黎曼零点位置的研究中出现过。这些不同的实验都与随机量子鼓的统计量完全吻合。但是我们也知道并不是所有的统计量都是完美匹配的。物理学家逐渐开始明白在第 N 个能级和第（$N+1000$）个能级之间的距离统计量，依赖于你是否考虑了量子台球的因素，或是仅仅简单地测量随机量子鼓的频率。

精通混沌理论和量子物理两门学科的专家之一是布里斯托大学的麦克尔·贝里爵士（Sir Michael Berry）。在奥德兹克注意到在黎曼零点的数差图与随机量子鼓的数差图之间的偏差之后，贝里最先明白这个偏差意味着混沌量子系统是解释素数行为的最佳物理模型。贝里是科学界中非常有魅力的一个人，他为自己的学科带来了更多的人情味，而这正是那些沉浸在科学世界中的人们所缺乏的。他是一位新古典主义人物，总喜欢引用一些文学巨匠和科学大师的言论来说服他人接受自己的世界观。他擅长于透过复杂数学公式的表象寻找到完美的结果，能得到这位



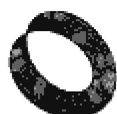
英国骑士的加盟，对于那些试图攻克黎曼假设的数学家而言，应该是一件很幸运的事。

自从20世纪80年代在《数学情报员》（*Mathematical Intelligencer*）杂志上读到一篇以“前5000万个素数”为题的文章之后，贝里就对素数产生了兴趣。这篇文章的作者是唐·查吉尔，就是那位曾经与邦比艾里就黎曼假设对赌的马普研究所的火枪手。在这篇文章中，查吉尔并没有单调地列出那数千万个素数，而是描述了这些黎曼世界中的零点是如何用来产生一些波，而利用这些波又可以奇妙地得到原先的结果，就是你一路数下去的素数个数。“这是一篇漂亮的文章，我认为黎曼零点是非常奇妙的东西。”贝里深深地着迷于黎曼假设的这个物理解释——这意味着素数中存在着音乐。

作为一位物理学家，贝里为素数领域带来了物理直觉，这是许多数学家缺乏的东西。数学家可以花很长时间在脑海中进行构思，但是他们忘记了在抽象数学世界与围绕我们的真实物理世界之间还有着许多联系。黎曼曾经将素数转化为波函数，对于像贝里这样的物理学家而言，这些波并非仅仅是抽象的音乐，而是可以转变为人人可听的物理声音。在贝里的关于黎曼假设的演讲中，他经常会使用黎曼音乐的录音——一种低沉的噪音。贝里描述它“有点像后现代音乐，但是感谢黎曼的工作，正如萧伯纳对瓦格纳所说的那样：音乐本身比听上去更妙。”

278

贝里对素数的兴趣来的正是时候，此时他对电子作为量子台球时的能级统计量与随机量子鼓的能级统计量之间的差别有了更进一步的理解。“我觉得把黎曼的零点和戴森的思想放在这个量子混沌的新联系之下再次审视，也许会发现有趣的结果。”贝里在量子台球能级中发现的统计量，会不会在黎曼 ζ 函数世界中的零点的统计量上有所体现呢？“我觉得看看这些零点是否真的具有这种方式的行为应该是一件不错的工作，于是我进行了一些大概的计算。”但是贝里没有足够的数据。“后来我听说了奥德兹克的事，他已经完成了这些伟大的计算。于是我写信给他。他给了我很多的帮助，他向我解释因为在某一点之后的计算会开



始出现偏差，因此他感到有点担心，担心自己肯定在计算中犯了错误。”

但是奥德兹克并没有物理学家的直觉。当贝里将这些零点和混沌量子台球的能级相比较时，他发现两者的匹配是完美的。奥德兹克发现的矛盾最终被证实是在随机量子鼓的频率统计量和混沌量子台球能级统计量之间的差别的首次发现。奥德兹克完全没有注意到这个新的混沌量子系统，但是贝里一下子就看出来了：

> 这是一个重要的时刻，因为结果显然是正确的。对我而言这是绝对令人信服的、完全的证据。如果你认为黎曼假设正确，那么在黎曼零点的背后不仅仅是一个量子系统，而是一个有着经典理论对应的、相对简单但是混沌的量子系统。这是一个愉快的时刻，它意味着，如果你愿意这么说，量子力学为黎曼零点的理论提供了工具。

有意思的是，如果素数的秘密真的隐藏在混沌量子台球游戏中，那么素数应该是可以用台球桌上的某个特殊路径来表示。某些路径在一段时间后，可以让台球回到它原先的起点，并且这个规律会循环出现。看上去这样的特殊路径正是代表了素数：每一条路径代表一个素数，路径回到自身需要的时间越长，所对应的素数就越大。

279

贝里的新方法最终融合了科学的三段伟大旋律：量子物理（极小世界的物理）、混沌（不可预测性的数学）和素数（算术的原子）。也许黎曼希望从素数中发现的规律只能用量子混沌来描述，在这一点上素数再次表明了自己谜一般的特征。在零点统计量和能级统计量之间的明显联系促使许多物理学家加入到寻找黎曼假设证明的队伍中来。最终也许会证实零点的起源确实是一个数学鼓，如果是那样，量子物理学家将是寻找这些鼓的最佳人选，他们的生命将因鼓声而产生回响。

现在我们的所有证据告诉我们黎曼零点是振动，但是我们不知道是什么造成了振动。也许振动的来源是完全数学的，没有任何物理模型。也许解释零点的数学会和解释量子混沌的数学相同，但是这并不意味着结果必须要有一个物理的表现形式。不过贝里并不同意这一点，他相信



一旦数学到位了,一定会有对应的物理模型,其能级可以反映黎曼零点。“对此我毫不怀疑,只要有人找出了零点的来源,一定就有人可以找出模型。”那这样的模型有没有可能已经存在,只是隐藏在宇宙的某个角落等待着我们去发现? 也许在卡尔·萨根《接触》一书中伊莉·阿若韦接收到的宇宙素数根本不是外星生命发来的信号,而只是某个振动的中子星发出的频率而已。就像贝里解释的那样,“正是由于众所周知的极权主义的法则,我们会认为只要是物理规则允许的东西都可以在别处自然地发现。我对这件事深表怀疑,当然你可以想办法将它虚构出来。”

奥德兹克有 AT&T 的资助, 贝里及其研究小组多年来也得到了另外一个大型商业机构的资助。惠普公司在英国布里斯托有一个主要机构,它们赞助了贝里研究小组的成员以获得量子物理的力量。惠普公司知道任何在黎曼假设方向上做出的进展, 都能加深我们对量子台球游戏的理解, 由于量子台球的规则可以帮助控制电脑中电路系统的行为, 理解电子在计算机芯片中刻出的凹槽上穿行的规律, 因此他们知道与这些顶尖量子台球选手保持同步的重要性。

280

42——终极问题的答案

尽管在经济低迷时期, 像 AT&T 和惠普这样的巨头都被迫削减了对素数的投入, 但仍有一家商业机构乐于为这种看上去是抽象游戏的研究进行投资。弗瑞电子（Fry Electronics）是一家在美国西部拥有大约 20 家大型电子商店的连锁机构, 主要为全国提供计算机配件和电子器件。当然这家公司提供的资助肯定比不上像 AT&T 和惠普这样的巨头, 但是如果你访问弗瑞电子在加州帕洛阿图的总部, 你会发现在商店的主入口旁边, 一扇破旧的铁门上挂着一个牌子——“美国数学研究所（American Institute of Mathematics）”。

研究所来自于公司董事约翰·弗瑞的想法。弗瑞和布瑞恩·孔瑞曾在圣克拉拉大学一起学习数学, 当孔瑞继续努力证明最多百分比的零点



落在黎曼临界线上，以便创下世界纪录时；弗瑞则从事着商业的投资活动，但是弗瑞并没有失去对数学的兴趣。当自己的电子公司获得了迅速发展之后，他开始思考是否有某种方法来支持这门学科。弗瑞已经赞助了一支五人制的足球队，因此他决定赞助一支数学队伍。

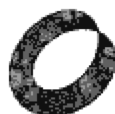
弗瑞联系到孔瑞，两人一起拟定了一个计划，决定集合大家的力量证明黎曼假设。为了实现这个计划，他们为一场计划于1996年在西雅图召开的纪念证明素数定理一百周年的会议提供了赞助。这并不仅仅是投入资金的事情——他们还希望能够鼓励新的合作风气。由于黎曼假设是人人都垂涎的东西，因此许多人都不愿意共享自己哪怕是最粗略的想法，以免为他人提供最关键的一步。孔瑞和弗瑞希望能打破这个怪圈，因为它将导致我们无法前进。会议或讨论班的重点就在于交流思想，即使最后不能得到任何结果。他们甚至让数学家围坐在圆桌前，像讨论商业计划那样进行交流。

在西雅图的会议上，出现了一些证据说明黎曼假设与量子混沌有关联。对仅仅通过观察两幅几乎无法分辨的图像得到的联系，一些数学家当场表达了自己的担心。其中提出一些有益怀疑的人是彼得·萨那克，尽管他深深惊讶于量子混沌和黎曼 ζ 函数零点之间的相似性，但是只有真正的联系才能令他信服。

281

萨那克是普林斯顿大学的领军人物之一。当安德鲁·怀尔斯秘密地向费马大定理发动进攻的时候，萨那克对他有着充分的信心。萨那克对于黎曼假设的兴趣来自于20世纪70年代中期，当时他刚从南非来到美国跟随保罗·科恩工作，地点就在弗瑞电子公司不远处的斯坦福大学。作为一个学生，萨那克选择科恩是因为他对数理逻辑有兴趣。在10多年前的1963年，科恩因为成功地利用逻辑推理解决了希尔伯特23问题中的第一问题而震惊世界。与希尔伯特期望得到的“是”或“否”的答案完全不同，科恩证明了对这个问题你可以“选择”你想要的答案。

这位南非学生来到斯坦福之后，认为自己应该研究差不多困难的逻辑谜题。但是科恩让他关注另外一道希尔伯特难题，第八问题。因为知



道解决希尔伯特第一问题是一件不可重复的行为，科恩认为只有解决黎曼假设才能给他带来比期望值更多的成就感。于是他将自己关于这个问题的想法与萨那克分享，并由此促成了萨那克对数论的终身热情。

萨那克对于这门学科的热情是具有传染性的。当他谈到数学时，空气中都弥漫着能量和兴奋。现在已经年老并且耳朵不太灵光的塞尔伯格说，萨那克是自己在普林斯顿少数几位能听清楚的数学家之一。当萨那克热情洋溢地讲述自己的新发现时，他那南非口音就会回荡在数学系的大楼中。人们都对量子物理进入到数论的神圣殿堂感到兴奋，但是萨那克关心的更多：是否有证据表明在能级和零点之间找到联系可以导致一些更实际的进展？

这种联系也许为我们指出该到何处去寻找解释，但是这种学科的交叉并没有告诉更多我们不知道的信息。它看上去只是基于不同统计量之间的匹配，看上去相似的两幅图像代表的事实并不能让数论学家相信，这就是他们所要找的联系的证据。毕竟，数学家仍然怀疑图像是否有能力揭示真相，尽管黎曼曾将几何学带入主流数学中。

萨那克参加了西雅图的会议，但是他认为抛开锐利的数学直觉没有什么可以揭示黎曼世界中的奇妙之处。在听到关于黎曼零点和量子混沌台球中能级相似性的报告，以及贝里播放的素数的音乐之后，萨那克再也不能忍受。看到两个领域的图像都出现同样的模式是很有意思的一件事，但是有谁能指出某些真正的素数理论结果是得益于这种联系呢？萨那克向在场的量子物理学家提出了挑战：用量子混沌和素数之间的相似性告诉我们一些关于黎曼世界的、我们不知道的结果——某些特殊的、除了统计量之外的结果。同样萨那克提供了一瓶好酒作为奖励。

282

感谢特殊数字 42 做出的重要贡献，贝里的学生乔恩·基廷（Jon Keating）最后赢得了萨那克的这瓶好酒。如果你对流行小说很熟悉，你也许会知道 42 这个数字有着特殊的意思。在道格拉斯·亚当斯（Doug-



las Adams）的《银河系搭车指南》[1] 中，扎泼德·比博布洛克斯（Zaphod Beeblebrox）发现42是关于生命、宇宙和万物的终极问题（即使这个问题的内容并不是很清楚）的答案。数字42同样是19世纪后半叶牛津的数学家刘易斯·卡罗尔（Lewis Carroll）的珍爱。在卡罗尔的《爱丽思漫游奇境》中，国王在审讯红心武士的时候宣布："根据第42条，所有身高一英里以上的人必须退出法庭。"在其他作品中刘易斯也多次用到了数字42，在《追猎蜗鲨》（*The Hunting of Snark*）中，海狸带来了"42个精心包扎好的箱子/每个箱子上面有着清晰的签名"。奇怪的是，这个数字居然也要进入黎曼假设的故事中，使那些持有怀疑态度的数论学家们信服，量子混沌是同一个素数硬币的另一面。

听说萨那克愿提供一瓶好酒之后，孔瑞为物理学家提出了一个非常特别的问题，作为检验的对象。这个问题一直盘旋在孔瑞的心中，因为它与孔瑞多年奋斗的目标有很大关系，但一直没有什么结果。黎曼 ζ 函数有一个特性称为它的矩（moments），利用矩可以生成一组数列。但是问题在于数学家对于如何计算出这组数列没有太多的信息。哈代和利特伍德曾经证明这列数中的第一个数是1，利特伍德的学生阿尔伯特·英格汉姆在20世纪20年代证明了下一个数是2。可是这些结果并没能发展下去，寻找到可供进一步探索的规律。

在西雅图会议之前，孔瑞已经与另外一个同事阿密特·古什（Amit Ghosh）在寻找下一个数的问题上做了大量工作，他们猜测数列中的第三个数将会是一个大的跳跃——42。对孔瑞而言，这个数成为序列中的下一个数"是相当令人惊讶的事，这意味着其中存在着一定程度的复杂性。"目前并没有对该序列下一个数的猜测。因此孔瑞为物理学家提出的挑战就是，用量子物理中的类似术语来解释42。对此孔瑞说："42是一个数，要么你的结果就是它，要么就不是。它与观测曲线之间的匹配

283

[1] *The Hitch Hiker's Guide to the Galaxy*，是道格拉斯·亚当姆斯的科幻小说代表作，2005年由博伟影业公司搬上大屏幕。



程度完全不同。"

乔恩·基廷在离开西雅图之后，立刻勇敢地投身到这个工作中去。由于这次会议很成功，弗瑞和孔瑞决定接着办第二次会议，它于两年之后在维也纳的薛定谔研究所召开。由于薛定谔是创立量子物理的先锋人物，选定这个会议地点也许是考虑到在数论和量子物理之间产生的新的合作关系。

与此同时，孔瑞得到了另外一位数学家史迪夫·高内克（Steve Gonek）的帮助。利用他们已知的数论知识，再加上大量的努力，他们终于可以猜测序列中的第四个数——24024。"于是我们得到这个数列：1，2，42，24024，…我们试图像狄更斯那样猜测这个数列是什么，但是我们知道自己的方法已经不能再向前推进了，因为对于下一个数它给出的答案是一个负数。"而已知的结果是序列中所有的数都是正数。孔瑞来到维也纳准备在会议上报告他们的猜测，序列中的下一个数是24024。

"基廷来得稍微晚了一些。在他将要做报告的那个下午我看见了他，他报告的题目令我很惊讶，一直在想他是不是真的得到了这个结果。当他一出现，我立刻走上去问他，'你真的将它算出来了吗?'他说是的，他真的得到了42。"实际上，基廷和他的研究生妮娜·斯乃思（Nina Snaith）找到了一个公式，据说可以生成序列中的所有数。"于是我告诉他24024的结果。"这是一次真正的测试，基廷和斯乃思的公式与孔瑞和高内克的猜测吻合吗？因为基廷事先知道自己要寻找的结果是42，因此他也许会对这个公式进行修改而得到42。但是24024这个数对于基廷而言是全新的，在这个数上他没法做手脚。

"就在乔恩作报告之前，我们走到薛定谔研究院的一块黑板旁，开始计算这个公式是否真的预测了这个序列中的第四个数。"他们不断地犯一些计算错误——在多年的抽象思维之后，数学家并不一定是心算高手，也许连童年学过的乘法表也会忘记。最终他们还是完成了计算，"当24024出现在最后的结果中时，那种感觉真是不可思议，"孔瑞回忆

284

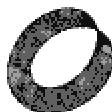
说。随后，基廷心中还带着与孔瑞和高内克的猜测完全一致的兴奋，迅速冲回报告厅进行演讲，这是他和斯乃思的公式首次向大众公布。基廷将那段在黑板前的经历描述为“我科学生涯中最兴奋的几秒钟”。

基廷曾经对在数论学家面前讲述自己的结果感到很不安，作为一个物理学家，他居然要向那些已经在此方向上工作过多年并且有着透彻理解的人讲述数论，但是24024给他的刺激充实了他的信心。当时已是此方向权威的塞尔伯格也坐在听众席中。基廷报告完毕之后是观众提问时间，以塞尔伯格的习惯，在报告结束时他并不是提出问题，而是以“我在50年代就得到了这个结果，”或者“我在30年前就试过这个方法但是它不管用。”之类的话语来给出自己的意见。基廷也做好准备迎接这一命运，然而塞尔伯格开始不断地提出问题，显然是被基廷的新想法所吸引。在基廷勇敢地回答完塞尔伯格的所有问题之后，塞尔伯格发表了自己的意见：“这肯定是正确的。”基廷赢了萨那克的挑战，告诉了数学家他们以前从不知道的事情。萨那克也按时地兑付了自己许诺的一瓶好酒。

黎曼零点和量子物理之间的相似性所表达出来的能力是双重的。首先，它告诉我们该到何处去寻找黎曼假设的答案；其次，正如基廷已经证明的那样，它可以预测某些黎曼世界的性质。贝里说过，“这个相似性并没有严格的数学基础，我们判断它究竟有多大的用处，只能是看它究竟能提供给数学家多少可以证明的东西。对此我没有什么不好意思——作为一个物理学家，我喜欢费曼的格言：‘我们知道的总比已证明的要多得多。’”即使物理学家无法给出一个能生成零点的物理模型，数学家也承认最终很有可能是物理学家证明了黎曼假设。这也是为什么在本书开始邦比艾里的愚人节玩笑中，那个故事如此可信的原因。

黎曼的最终方法

物理学家相信黎曼零点落在一条直线上的理由是，它们可以生成某



个数学鼓的频率。落在线外的零点对应的是一个虚频率，这是被理论禁止的。这样的论断已经不是首次被用来解决问题。基廷、贝里和其他一些物理学家在学生时代就知道一个流体力学的经典问题，其结论依赖于同样的推理。这个问题讨论的是一个旋转的流体球，它由其中粒子之间的相互作用力聚合在一起。比如说，恒星就是一个旋转的气体球，它自身的重力保证了它的形状。现在问题是，如果你轻轻地踢一下这个旋转流体球，会发生什么事情？是这个流体球变得摇晃不定但仍然保持自身形状，还是这一踢会破坏整个球的完整性？这个结果依赖于证明为什么某些虚数会落在同一条直线上。如果它们确实落在同一直线上，旋转流体球将保持原来的完整性。而这些虚数实际上排成一条直线的原因与量子物理学家关于证明黎曼假设的思想非常接近。谁发现了这个结果？谁利用了振动数学来迫使这些虚数落在一条直线上？除了黎曼没有别人。

285

在薛定谔研究院获得成功之后不久，基廷被邀请去往哥廷根，讲授关于如何利用黎曼假设与量子物理之间的联系来研究黎曼假设的内容。大部分路过哥廷根的数学家都会去那里的图书馆，阅读黎曼那些未发表的手稿。不仅仅因为这是一种难得的与数学史上如此著名人物发生联系的经验，更多的是因为在手稿中仍然有许多未解之谜被隐藏在黎曼潦草的字迹中。手稿就相当于数学中的罗塞塔石碑①。

在基廷出发去哥廷根之前，一位数学系的同事菲利普·德拉金(Philip Drazin)建议他同时查看一下黎曼解决经典流体力学问题的那部分手稿。虽然黎曼的管家烧毁了他的大部分文章，但是手稿中仍然包括了丰富的内容。这些手稿按黎曼生活的不同时期和他的不同兴趣分成许多卷。

在哥廷根的图书馆里，基廷索阅了自己希望查阅的两部分手稿：其一是黎曼关于 ζ 函数世界中零点思想的手稿，另一份就是黎曼关于流体

---

① The Rosetta Stone，1799 年拿破仑侵略埃及时在尼罗河三角洲西部小镇拉希德(Rashid)发现的一块黑色玄武石板。其上以希腊语、通俗语和象形文字三种文字记载着托勒密五世时期的法令，经过英国物理学家托马斯·杨和法国古埃及学家商博良的努力，成功地利用罗塞塔石碑破译了古埃及文字。



力学的工作手稿。由于从储藏室送来的手稿只有一堆，基廷忍不住提醒馆员他索取的是两部分的手稿，两“部分”内容在同一堆手稿中，馆员这样告诉他。当基廷浏览这些手稿时，惊讶地发现黎曼在构思关于旋转流体球的证明的同时，也在考虑那些ζ函数世界中位于海平面的点。现代物理学家打算用来迫使黎曼零点成一直线的方法已经被黎曼用来解决了流体力学中的问题。在基廷面前的同一堆手稿中，有着黎曼对两个问题的思考。

286

再一次的，手稿显示了黎曼是多么领先于他的同时代人。他也许没有意识到自己解决的这个流体力学问题的重要性，但是他的方法却告诉我们，为什么在分析流体球时出现的某些虚数都落在同一直线上。同时，在同一份手稿中，他试图证明为什么在他的ζ函数世界中所有的零点都落在一条直线上。在发现素数和流体力学的新结果之后几年，他将自己的新思想记录在一个黑色封面的日记中，但是令人恼怒的是，这本日记并没有留下来。与这本日记同时消失的，是黎曼关于如何将这两个从数论和物理产生的主题结合起来的思想。

在黎曼去世后的数十年内，数学和物理开始各行其道。虽然黎曼很乐意将两门学科联合起来考虑，但是逐渐地在他之后的科学家对两门学科的交叉表现出很少的兴趣。只有到了20世纪物理和数学才又回到并肩工作的情形，也许正是这种重聚才导致了黎曼所期望的突破。

虽然这些与物理学的联系令人兴奋，许多数学家仍然相信以自身学科的能力，足以解决这个素数难题。许多人同意萨那克的观点，认为黎曼假设的答案位于数学的核心深处。这种认为数学本身可以解决问题的想法可以追溯到20世纪40年代，一位相当特殊的法国囚犯的活动。

287



第十二章

拼图玩具中消失的一片

> 有人说数学的历史应该类似于对交响曲进行音乐分析的步骤。乐曲中有许多主题，或多或少你可以发现某一个主题首次出现，随后它会与其他主题混合在一起。作曲家的水平就在于他能同时处理这些主题，有时小提琴演奏一个主题，长笛演奏另一个主题，然后两个主题交换并将乐曲向前推进。数学的历史同样如此。
>
> ——安德烈·魏伊（André Weil），《数论二讲，过去和现在》

量子台球游戏也许可以解释黎曼假设，但抛开这一切带来的兴奋，许多数学家仍然对闯入纯粹数论世界的物理学家持有怀疑态度。其中大部分人相信自己学科的能力足以解释为什么素数的行为像我们相信的那样。也许同一种类型的数学既能解释量子现象又能解释素数的观点听上去有点道理，但是许多数学家觉得物理直觉能帮助证明黎曼假设这个想法根本靠不住。当人们开始传说纯数学理论最成功的建筑师开始把注意力转到黎曼假设上来时，数学家的自信看起来得到了支持。阿兰·科纳从 20 世纪 90 年代中期开始就自己对答案的想法作了一些演讲，许多人觉得解决黎曼假设的时刻终于到来了。

科纳迎面狙击黎曼假设的事实就其本身来说也是值得注意的。拿塞尔伯格来说，他自己承认从来没有真正试着去证明黎曼假设。他说，如果你连战斗的武器都没有，那怎么能上战场呢。科纳这样描述自己参战的决定，“用我第一个老师古斯塔夫·周魁（Gustave Choquet）的话讲，



一个人公开面对知名的未解难题，冒着因失败而被别人记住的风险，总比其他人要强吧。在到达一定年纪之后，我意识到'安全地'等待直到生命的终点无异于另一种方式的击败自我。"

由于科纳已经在数学的其他领域解决了不少难题，因此看起来他有能力获得更强有力的技术。他开创的一个方向叫做非交换几何，现在被认为是黎曼几何的现代版本，而黎曼几何曾在19世纪的数学进程中产生过深远的影响。就像黎曼的工作为爱因斯坦相对论理论的突破铺平了道路，科纳的非交换几何也提供了一套强大的语言，利用它可以更好地理解量子物理世界的复杂性。

288

科纳创造的新数学被认为是20世纪数学的一个里程碑，因此他在1983年获得菲尔兹奖。但是科纳的新语言并不是凭空出现的：它是开始于"二战"期间的法国数学复兴的一部分。当逃离欧洲迫害的知识分子流入普林斯顿，并促成了研究院的壮大之时，科纳是法国一所成立于20世纪50年代的研究院的教授。这个研究院的成立是为了帮助巴黎重新成为数学舞台的中心，在拿破仑统治期间，哥廷根取代了巴黎的中心位置。

科纳的思想代表着某种数学运动，希望用非常复杂并且抽象的观点来看这门学科。在过去的50年里，数学使用的语言已经经历过一次进化，并且还将继续进化下去。许多人相信在这个过程完成之前，我们将不会有一种足够先进的语言来精确地解释为什么素数的行为正如黎曼假设预测的那样。这次新的法国数学革命的源头是第二次世界大战期间法国的一间牢房，从这间牢房中产生了一种新的数学语言，一种即将在黎曼为了理解素数而构建的世界里发挥探索能力的语言。

会多种语言的人

在1940年，时任著名法国杂志《法国科学院院报》（*Comptes Rendus*）编辑的伊利·卡当（Elie Cartan）收到一封写给自己的信。自从19



世纪初，柯西在《院报》上发表关于虚数数学的经典文章以来，《院报》就成了做出激动新结果之后发表声明的首选杂志。令卡当感到有趣的是这封信的寄件人地址：鲁恩市波恩-鲁外尔军事监狱（Bonne-Nouvelle Military Prison，Rouen）。如果不是卡当认出了信封上的笔迹，也许这封信就要被扔到一边，被当作是哪个疯子寄来的宣称证明费马大定理的信件。笔迹属于一位名叫安德烈·魏伊的数学家。当时魏伊已经作为法国年轻的数学新星获得了一定的声望，卡当知道魏伊的东西还是值得看一看的。

289

当卡当打开这封信之后，其内容给他带来的惊讶远远大过于从监狱收到一篇文章的惊讶。魏伊找到了一种方法，可以证明为什么在某些世界中位于海平面的点总倾向于落在同一直线上。虽然这个技巧对黎曼世界并不适用，但是它对其他世界适用的事实已经足够让卡当相信其中肯定有某些重要的东西。此后魏伊的定理成为数学家寻找黎曼假设证明的路途中的灯塔，科纳的成果也要部分地归功于魏伊在鲁恩监狱中提出的这个思想。

魏伊拥有的可以遨游于这些世界而别人没有的能力可以追溯到他早期对古代语言的热爱，特别是梵语。他相信新的数学思想的发展与语言的复杂形式的发展是相一致的。对魏伊而言，无论是在印度，语法的发明要先于十进制和负数的发明；还是在中世纪，阿拉伯的代数从阿拉伯语言的复杂发展中脱胎而出，都没有什么惊奇可言。

魏伊强大的语言能力赋予他非凡的能量创造出了一种新的数学语言，从而可以让他将那些一直无法说清楚的细微之处清晰地表达出来。但是也正是他对于语言的迷恋，特别是他对古代梵文作品《摩诃婆罗多》的热爱，让这位杰出的年轻数学家在1940年初被捕入狱。

魏伊的数学才能在他童年时期就已表现出来。他的第一个老师说自己的这个6岁的学生，“不管我告诉他什么方面的知识，他好像都知道。”他的母亲知道如果自己的儿子总是在班里名列前茅就不可能得到足够的智力发展，于是她找到校长坚持让年轻的安德烈转到高年级就

读。惊讶的校长这样回答她："夫人，这是第一次一位母亲在我面前抱怨自己儿子在班级里的名次太高。"感谢这位热心的母亲，安德烈被调到了孟贝先生（Monsieur Monbeig）的班级。

孟贝先生有一套不寻常的教学方法，魏伊认为多亏了这套方法才培养自己成为了数学家。比如说，这位先生并不是让学生死记硬背那些语法，而是精心制作了一套个人的代数记号系统来揭示语法中潜藏的规律。在后来的日子里，当魏伊看到诺姆·乔姆斯基（Noam Chomsky）革命性的语言思想时，对他而言根本没有什么新东西。魏伊意识到"这些早年利用非平凡符号体系进行的练习肯定具有非常大的教育价值，特别是对未来的数学家而言。"

290

因此数学成为了魏伊的追求和爱好，"只要我摔倒在地，我的妹妹西蒙妮就会不假思索地跑去拿来我的代数书安慰我。"最终魏伊的才能被法国伟大的传奇数学家雅格斯·哈达马发现，哈达马在世纪之交的时候因为证明了高斯的素数定理而名扬世界。哈达马鼓励魏伊继续追求数学，在魏伊 16 岁的时候，他进入了成立于法国大革命期间的巴黎高等师范学院（École Normale Supérieure），开始接受成为职业数学家的训练。

在高等师范学院学习数学的同时，魏伊继续沉迷于古代语言之中。这一爱好后来变成了一个新的数学世界。但是在那时魏伊只是希望可以读懂用原文书写的希腊和印度的古典史诗。有一篇史诗曾相伴他一生：薄伽梵歌[①]，摩诃婆罗多中关于神的诗歌。在巴黎的时候，魏伊用来学习梵文的时间不亚于用来学习数学的时间。

不仅仅是史诗，魏伊相信要了解任何文字中全部的美，唯一的方法就是读原文。同样在数学中，他也强调要回去阅读那些大师原始的文章，而不能依赖于对其工作的二次转述。"我深信人类历史上最有价

---

① Bhagavad-Gita，并入摩诃婆罗多的印度教经文，古梵语史诗。以哲学对话的形式写成，是克里希纳对阿朱那王子在道德和神的存在本质方面的教导。



值的就是那些真正伟大的思想，而真正可以了解这些思想的唯一方法就是直接与他们的著作交流，”他在自己的自传《一个数学家的学徒历程》（*The Apprenticeship of a Mathematician*）中这样写道。这也是他为什么会去研究黎曼著作的原因，“我一直都很感谢由于意外的好运而开始的这项工作，”从此关于素数本质的黎曼假设贯穿了魏伊的全部数学生命。

当魏伊通过了高等师范学院的考试之后，他仍然小于法定强制兵役的年龄，因此他开始了一场环游欧洲的数学之旅。他穿越了整个欧洲大陆——米兰、哥本哈根、柏林、斯德哥尔摩——听取别人的演讲，与当时数学界的先驱交谈。在当时还未受到希特勒校园净化运动的哥廷根，魏伊将脑中的思想综合起来构成了他博士论文的基础。在三位欧洲最著名数学家——高斯、黎曼和希尔伯特——的根据地，魏伊意识到巴黎已经明显失去了它的数学地位，那曾经在傅里叶和柯西时代享受到的辉煌。这部分的是因为大部分本该在20世纪30年代成为知名人物的法国数学家都在第一次世界大战中丧失了他们的生命，这也造成了一代的缺失。另外在战后的日子里，很少有德国的著名人物来巴黎讲授他们的工作，从而造成这座城市新思想的匮乏。从费马以来的伟大法国数学传统将会发生什么样的改变？魏伊和一群年轻的数学家决定用自己的双手来改变这一切。

291

由于这群有志青年中没有人是领袖人物，因此他们创造了一个名字：尼古拉斯·布尔巴基（Nicolas Bourbaki）。利用这个笔名他们编写了一部反映当时数学现状的著作。他们的指导思想来源于那些使得数学成为一门独特科学的观念。数学是一座大厦，它构建在公理之上，在数学中古希腊人证明的定理仍然是21世纪数学中的定理。于是布尔巴基小组开始研究数学大厦现在的状况，并且用现代数学的语言写出一份全面的总结。受到影响了整个西方数学2000多年的欧几里得经典巨著的启发，他们将自己的著作命名为《数学原理》（*Elements de Mathematique*）。抛开这个希腊传统，这本书具有完全的法国特点。原本发展数



学的目的是为了解决特定的问题，而这本书强调的是最广泛的内容以及所有可能的任何结果，即使这样意味着忽略了数学原本的特性，那他们也在所不惜。

实际上“尼古拉斯·布尔巴基”是一个少为人知的法国将军的名字，他们选择这个名字的初衷是为了让自己的作品符合一个传统。在20世纪初的高等师范学院，一年级新生会参加一次特别的开学典礼，在典礼上高年级学生装作一位著名的外国来访者进行著名数学定理的讲演。讲演者会事先将某些错误安排到一些定理的证明中，新生们必须能指出这些错误。而线索就在于，这些包含错误的定理往往都是以一些不出名的法国将军来命名，而不是它们原先的发现者。

这些年轻法国数学家的集会完全是无组织的、混乱的场面。对此一位创始人让·迪奥多内（Jean Dieudonné）将其描述为“如果外人被邀请参加布尔巴基学派的会议，那么他的评论肯定是，这是一群疯子的聚会。他们不能想象这些常常是三个或四个人同时大喊大叫的年轻人居然能做出某些有才智的结果。”布尔巴基学派的成员相信，正是这种无组织的特点才是这个计划能照常运转的关键。也正是在他们争论着希望统一当时的数学时，魏伊后来发展的新语言开始有了萌芽。

292

1930年，魏伊对古代语言和梵文的热爱为他获得了第一份工作，离德里不远的阿里格尔穆斯林大学的教授职位。该大学本希望让魏伊讲授法国文化，但是最终决定让他教数学。在印度的日子里，魏伊见到了甘地。甘地哲学的熏陶和他所读的薄伽梵歌的影响，在他回到酝酿着战争的欧洲之后，给他带来了致命的后果。在薄伽梵歌中，克里希纳建议阿朱那应该按照他个人的行为准则（dharma）来处世。而阿朱那是一名武士，这就意味着除了不可避免的毁灭之外都应该战斗。可是魏伊觉得自己的行为准则在告诉自己相反的一面——坚持自己的和平主义信念。于是他下定决心，如果战争爆发，他将逃到某个中立国以避免法国军队的征兵令。

在1939年夏天，魏伊和妻子作为旅游者来到芬兰，他希望芬兰将



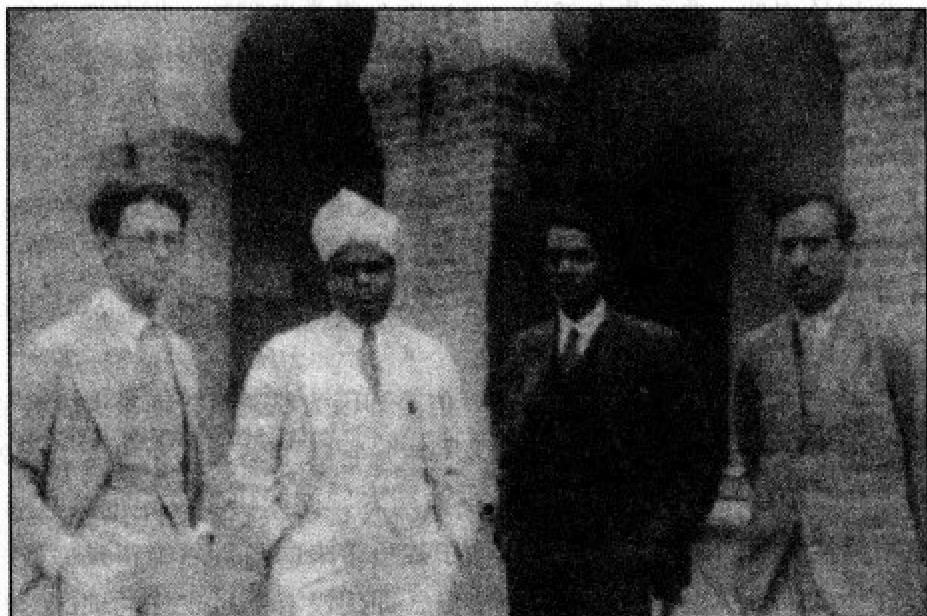


图 44　安德烈·魏伊（1906～1998）在印度的阿里格尔，以及维加雅拉伽樊（魏伊身旁的那位）和他的两个学生，摄于 1931 年

是一块合适的跳板，以便于他将来逃往美洲，可是事实证明这是一个巨大的错误。在 1939 年 8 月 23 日夜，斯大林签署了苏德互不侵犯条约，这意味着前苏联和德国结盟。作为中立的交换条件，希特勒向斯大林保证不干涉前苏联在爱沙尼亚、拉脱维亚、东波兰和芬兰的行动。1939 年 9 月战争爆发，芬兰政府明白自己的国家不久也将卷入战争，因此任何与前苏联的联系都被认为是极端可疑的。因此，当政府发现一封由法国旅游者寄往前苏联地址的信件，并且其中满是无法理解的公式时，他们很快认为这个旅游者是为敌人工作的。1939 年 12 月，这位法国人被以莫斯科间谍的名义逮捕。就在他要被执行处决的前一天晚上，警察局长去参加一场晚宴，结果发现自己身边坐着的是一位来自赫尔辛基大学的数学家罗尔夫·内凡林纳（Rolf Nevanlinna）。

293

在喝咖啡的时候，警察局长问内凡林纳，“明天我们要处决一个间



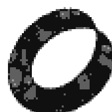
课，他说认识您。通常我不会因为这样的小事来麻烦您，但是既然今天碰到您了，我很高兴有这个机会向您咨询一下。”“他叫什么名字？”内凡林纳问。“安德烈·魏伊，”警察局长回答道。内凡林纳大吃一惊，因为在刚过去的夏天里他曾于自己位于乡下湖边的住所招待过魏伊和他的妻子。“真的需要处决他吗？”内凡林纳请求道，“你们不能将他护送到边境然后驱逐他吗？”“恩，这个方法也不错，我倒是没有想过。”由于这次幸运的晚餐，魏伊躲过了一颗子弹，而数学界也没有损失20世纪一位伟大的专家。

1940年2月，魏伊回到了法国，但是却因为躲避兵役而被关在鲁恩的监狱中等待着审判。数学的乐趣之一就是它除了笔、纸和想象力之外不再需要其他的工具。监狱可以提供前两者，而魏伊有充足的第三者。塞尔伯格在挪威的时候，就曾觉得由于战争带来的与世隔绝正是做数学的最佳环境。而作为印度的一位办事员，即使没有受过正规的训练，拉马努扬仍然做出了丰硕的成果。哈代的一位学生、魏伊在印度的同事维加雅拉伽樊（Vijayaraghavan）曾对魏伊开玩笑地说，“如果我可以有6个月或者一年的时间呆在监狱里，也许我就能证出黎曼假设了。”现在，魏伊得到了检验维加雅拉伽樊理论的机会。

黎曼曾经为我们构建了一个世界，其中那些位于海平面的点蕴含着素数行为的秘密。为了证明黎曼假设，魏伊需要证明为什么这些海平面上的点会排列在一条直线上。他想了好几个办法来探索黎曼世界，但是都没有成功。自从黎曼发现了素数和ζ函数世界的虫洞以来，数学家已经遇到过不少相似的世界，可以用来解释数论中的其他问题。这些由ζ函数的变体所定义的不同世界的能力，为它们获得了几乎是狂热崇拜的地位。它们成为了数论中几乎无所不在的东西，以至于塞尔伯格曾倡议要设立一个不扩散条约来防止ζ函数的滥用。

294

正是在探索某个相似的函数世界时，魏伊发现了一种方法，可以解释为什么这些位于海平面的点总是倾向于排成一条直线。魏伊探索的函数世界与素数没有关系，但是却是解决类似于$y^2 = x^3 - x$这样方程在某



个高斯时钟计算器上有多少根的关键。举例来说，在一个五小时的时钟计算器上，如果将 $x=2$ 代入方程的右端，就可以得到 $2^3-2=8-2=6$，这在五小时的时钟计算器上是1；类似的，取 $y=4$ 代入方程的左端，可以得到16，它在五小时的时钟计算器上同样是1。因此，我们就可以得到答案 $(x,y)=(2,4)$，这样的一组数称为方程的一个解，因为将它们代入方程，并在五小时的时钟计算器上进行计算之后，方程的两端相等。实际上，对于 (x,y) 我们有7种不同的选择可以使得方程成立：

$$(x,y)=(0,0),(1,0),(2,1),(2,4),(3,2),(3,3),(4,0)$$

如果我们选择另外一个不同的素数时钟，比如说 p 小时的素数时钟，情况会怎样？此时满足方程的解的个数大约是 p，但是并不恰好是 p。就像高斯对素数个数的对数估计，总是在真实素数个数的附近波动，因此 p 有可能是过高或过低地估计了真实解的个数。实际上，正是高斯——在其数学日记的最后一页上——首次证明了对这个特定方程，估计的误差不会超过 p 的平方根的两倍。对于这个方程高斯使用了一种特别的方法，但是无法适用于其他方程。而魏伊证明的优美性就在于它适用于任何由 x 和 y 构成的方程。通过证明了每个方程的 ζ 函数世界中位于海平面的点均排成一直线后，魏伊推广了高斯的发现，估计的误差实际上不可能超过 p 的平方根。

虽然这与黎曼假设没有任何直接的联系，但魏伊的证明仍然是心理上的重要突破。他找到了一个方法，可以证明由类似于 $y^2=x^3-x$ 这样的方程生成的函数世界中位于海平面的点都落在同一条直线上。因此，当卡当打开魏伊的包裹并看到其中的证明时，他不可能不兴奋，因为他想象到也许这些新的技巧可以搞清楚黎曼原先世界中的秘密。

295

对于理解方程的解，魏伊已经走出了通往一门全新语言的第一步。魏伊早年在欧洲游学的时候就已经知道，在罗马由弗朗西丝柯·塞维里（Francesco Severi）和古伊多·卡斯特诺渥（Guido Castelnuovo）带领的一些意大利数学家已经做过类似的东西。但是这些意大利人的基础明显不够坚实，无法支撑魏伊需要的数学。魏伊的思想成为后来我们称为代



数几何（Algebraic Geometry）这门学科的基础，而费马大定理证明的核心也正是代数几何。

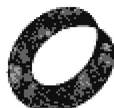
利用这种新的语言，魏伊可以为每个方程建立一组非常特殊的数学鼓。它不同于物理鼓中无穷多的频率，也不同于量子物理中无穷多的能级，它只有有限个频率。魏伊鼓的频率准确地标记出方程对应的函数世界中位于海平面的点的坐标，但是他仍需要做进一步的工作以保证这些点落在同一直线上。在前文中频率对应着量子物理中的能级，一个零点落在临界线外代表着虚能级的出现，这是被物理理论所禁止的。但是此时这种情况不再成立，因此魏伊需要找到另外的东西来让这些零点落在同一直线上。

当魏伊呆在自己的小牢房中，倾听自己构造的鼓的声音时，他突然明白自己已经拥有了拼图玩具中的最后一片，可以解释为什么这个鼓的频率会落在同一条直线上。当他作为一名研究生游学欧洲时，他学过一个由古伊多·卡斯特诺渥推导出的定理，现在这个定理是让这些方程对应函数世界中的零点以一种规则的方式排成一直线的关键之处。如果不是幸运地想起卡斯特诺渥提供的这个结果，这些世界将和黎曼世界一样仍然无法接近。普林斯顿的彼得·萨那克承认，“魏伊能成功地证明这些结果，在某种意义上而言是一个奇迹。”

魏伊部分成功地实现了维加雅拉伽樊的梦想。他也许没有能攻克素数的黎曼假设，但是他找到了一种方法证明了在相关的函数世界中位于海平面的点总是倾向于落在同一直线上。魏伊在1940年4月7日写信给自己的妻子埃弗琳，“我的数学工作进展远远超过我的预想，但是我也有一点担心——如果只有在监狱中我才能做得如此好，那是不是意味着每年我都得设法让自己被关起来两到三个月?”通常魏伊在发表结果之前总是要等上一段时间，但是由于未来很不确定，他又不敢冒险等待，因此他将自己的结果整理后寄给了《院报》编辑伊利·卡当。

296

魏伊在给妻子的信中谈到了这篇文章，“我对这篇文章非常满意，特别是因为它的写作地点（它肯定是数学史上的第一篇），还因为这是

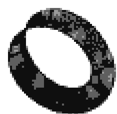


一个不错的方法，可以让我全世界的朋友知道我还活着，同时我也因为这个定理的优美性而激动得发抖。”读到这篇文章之后，魏伊同时代的数学家及朋友，伊利·卡当的儿子亨利·卡当（Henri Cartan）写了一封忌妒的回信：“我们都没有你那样幸运，可以待在一个不被打扰的地方工作……”

老卡当由于过度高兴而没能及时发表这篇文章。1940 年 5 月 3 日，魏伊多产的牢狱生涯走到了尽头。尽管卡当出庭为魏伊作证，但魏伊描述当时的情形像一场“相当差的喜剧”。最后魏伊因为没有按时服兵役而被判 5 年徒刑，但是如果魏伊愿意参军服务，判决可以延期执行。尽管在鲁恩监狱的时光里有着源源不断的数学灵感，魏伊仍然同意参军。事实证明这是一个明智的选择。一个月后，当德国发动进攻的时候，鲁恩监狱中的所有囚犯都被法国处死，因为这样可以加速监狱长的撤退。

利用一份从英国得到的伪造的医院证明，魏伊在 1941 年以肺炎名义退伍。魏伊设法为自己和全家弄到签证来到了美国，在美国他碰到了普林斯顿高等研究院的西格尔。在魏伊游学欧洲时，曾与西格尔成为好朋友。当西格尔去钻研黎曼未发表的手稿，并从中发现黎曼的秘密公式时，魏伊一直陪伴着他。西格尔很希望了解魏伊在类似函数世界中的成功是否可以用来理解黎曼原先的函数世界。

像西格尔一样，许多人都相信不管是什么使得魏伊在其他函数世界中获得了成功，它总能为搜寻黎曼假设这一终极圣杯提供关键的线索。魏伊花了许多年寻找与黎曼世界的微妙联系，不幸的是，作为一个自由人他再没能做出他在鲁恩监狱中取得的那些成就。当魏伊在晚年描述自己对重温首次发现经历的渴望时，其中的忧郁之情溢于言表：“每个称得上数学家的人都经历过……那种兴奋的状态，在其中新的想法一个接一个，就像奇迹一般……这样的感觉有时可以持续数小时，甚至是数天。一旦你经历过，你就会渴望再次经历，但是它并非随你的意愿而来，而是从艰苦的工作中来……”



297

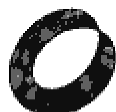
在1979年接受*La Science*①杂志的一次采访中，当被问到最希望证明哪个定理时，魏伊的回答是“在过去我有时想，如果我能证明1859年提出的黎曼假设，我将一直将它保留到1959年百年纪念的时候公布于众。”但是经过一些努力之后，并没有任何结果。“自从1959年以来，我觉得自己已经离它很远了，我逐渐地放弃了它，并非毫无遗憾。”

在其一生中，魏伊与志村五郎（Goro Shimura）有着密切的联系。作为一名日本数学家，志村五郎提出的一个猜想被安德鲁·怀尔斯在攻克费马大定理的时候解决。志村回忆魏伊曾在晚年向他承认，“我希望见到黎曼假设在我去世之前被解决，但是这不太可能。”志村记得他们曾经在一次对话中谈到查理·卓别林，在年轻时，卓别林咨询过一位算命师，算命师准确地预测到了他的未来。魏伊开玩笑说，“恩，那在我的自传中我也许会写，当我年轻的时候，一位算命师告诉我，我永远也无法解决黎曼假设。”

尽管魏伊希望证明黎曼假设、或至少是目睹它被解决的愿望没有实现，但毫无疑问他的工作非常重要。魏伊的证明给了数学家一定的信心，相信黎曼假设可以被证明，同样也帮助他们相信黎曼的直觉也许是正确的。如果在某个ζ函数世界中位于海平面的点都排成直线，那么素数的世界中这些点就有希望排成直线。不仅如此，在魏伊使用了某个奇怪的数学鼓来研究这些函数世界之后不久，量子混沌就告诉我们通过这样的方法也许可以找到答案。正如彼得·萨那克所说，“魏伊的结果是我们解决黎曼假设的灯塔。”

魏伊的新数学语言——代数几何——使得他能够清晰地表达出方程的解的细微之处，这在以往是根本不可能的。但是如果有任何能够推广魏伊思想来证明黎曼假设的希望，那么这必须在他于鲁恩监狱中做出的基础之上有新的发展。正是另一位来自巴黎的数学家为魏伊开创的新语

① 《科学美国人》杂志的法文版。



言带来了生命。完成任务的这位数学建筑大师是20世纪最奇特也是最富革命性的数学家——亚历山大·格罗腾迪克（Alexandre Grothendieck）。

298

新的法国革命

拿破仑在实施自己的学术革命之时曾创办了一些学校，像高等综合理工学院、高等师范学院等。但由于过分强调数学必须服务于国家需要，使得巴黎失去了数学活动中心的地位，让位于中世纪小镇哥廷根，在那里高斯和黎曼的抽象方法被允许进一步的发展。在20世纪后半叶，法国开始弥漫着乐观的气氛，觉得巴黎可以重新获得作为数学世界重要参与者的地位。

在布尔巴基学派主要人物的学术指导之下，一位俄国移民实业家、非常热爱科学的雷昂·默尚（Léon Motchane）发起并成立了一所新的研究所，它以成功的普林斯顿高等研究院作为参考，不同于拿破仑建立的那些学院，这所新的研究院是独立于政府之外的。由私人企业出资的法国高等科学研究院（IHES，Institut des Hautes Études Scientifiques）成立于1958年，它的地点坐落于离巴黎不远的一个名叫Bois-Marie的树木丛生的地区。经过这么多年，它已经成功地实现了创始人的梦想。研究院的前任院长马赛尔·布瓦特（Marcel Boiteux）将研究院描述为"充满热量的壁炉，繁忙的蜂房，一座修道院，在那里每个深埋的种子都有自己的土地可以生根发芽直至生长成熟。"研究院任命的首位教授是年轻的数学新星亚历山大·格罗腾迪克，这第一颗种子将以最壮观的方式开花结果。

格罗腾迪克是一位朴素的数学家，他在研究院的办公室中除了一幅他父亲的油画之外空空荡荡。他的父亲在1942年被杀死，在被送往奥斯威辛之前，一位同屋的舍友为他父亲画了这幅画。与肖像中的父亲一样，格罗腾迪克拥有同样炯炯有神的眼睛。



尽管他对自己的父亲了解不多，但是他母亲对他讲述过的父亲的故事还是带给他深远的影响。有一次他提到，自己的父亲应该是1900到1940年之间欧洲革命的真正名人：在1917年的十月革命中担任过领导者；和纳粹在柏林街头发生过武装冲突；在西班牙内战中服务于无政府武装。最终他在法国被捕，维希政府将他作为犹太人移交给纳粹。

299 格罗腾迪克自身的革命并不是发生在政治舞台上，而是发生在数学舞台上。从魏伊的初步尝试出发，他开始发展一套新的数学语言，如同黎曼的洞察力标志着数学的转折点一样，格罗腾迪克关于几何和代数的新语言标志着一门全新论证方法的产生，这套方法可以精确地表达出以往无法表达的思想。在18世纪末期数学家最终接受了虚数的概念，从而为数学打开了一片新的天地，而格罗腾迪克的这种新观点完全可以与之相媲美。但是这套新语言并不容易掌握，即使是魏伊也对格罗腾迪克开创的新的抽象世界感到不安。

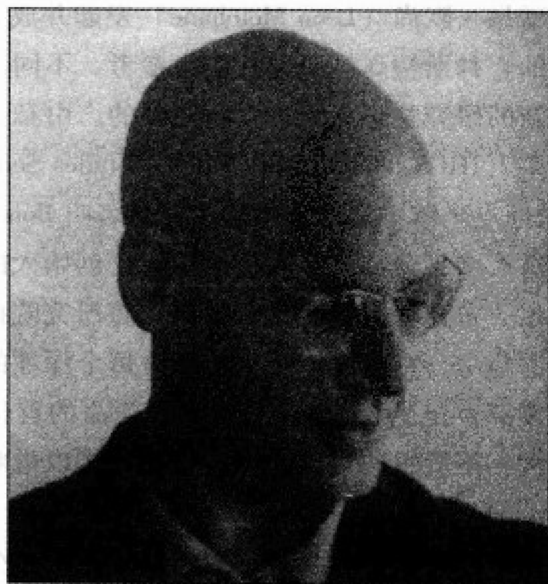


图45　亚历山大·格罗腾迪克，法国高等科学研究院教授，1970年离职

法国高等科学研究院自然而然地成为了布尔巴基学派的根据地，他



300

们仍然继续忙于写作关于现代数学的百科全书。格罗腾迪克也成为了其中一位主要贡献者。由于学派中的高级成员已经年届50，他们从布尔巴基学派中退出，以保证有年轻的法国新鲜血液来填补他们的位置。抛开别的不谈，正是布尔巴基的著作帮助法国重新获得数学世界的中心地位。在许多数学家的心中，布尔巴基都被看作是一个人，甚至还申请成为了美国数学会的成员。

许多法国之外的人批评布尔巴基对数学的影响，认为他在写作的内容方面是有选择性的。他们觉得布尔巴基将数学呈现为一门已完成的作品，而不是一个正在发展的有机体，从而消除了数学研究的活力；同时，布尔巴基为了强调广泛的选择而忽略了本学科那些奇妙但往往是很特殊的观点。但是布尔巴基认为自己的计划被人误解了，署名布尔巴基的著作是为了证实我们拥有的位置的稳固性。这些著作象征着新时代的《几何原本》，是欧几里得在2000多年前提供给我们的巨著的现实等价物。

传统的守护者、那些活跃在“二战”前的数学家开始抱怨说，他们不再认识那些自己已经工作多年的学科。西格尔就曾对用这种新语言表述自己的工作进行过评论：

> 我很讨厌用这种方式来描述我对这门学科的贡献，所有的东西都变得难看和难以理解。整个形式……完全矛盾于我们崇拜的数论大师——拉格朗日、高斯，或者小范围内的哈代、朗道——的工作带来的简单性和直观性。我仿佛看见了一头猪闯入了美丽的花园，践踏着所有的花花草草。

西格尔面对这样的抽象，表达了自己对数学未来的悲观态度：“如果现在这种无意义的抽象趋势——我称呼它为：空集的理论——不能被阻止的话，我担心在世纪末数学就将消亡。”

这是一个普遍存在的观念。塞尔伯格在听过一场关于也许可以证明黎曼假设的抽象框架提纲的报告之后，表达了同样的感受，“我的想法是，幸好这些讲座没有在更早的时候出现。我在讲座之后跟别人说了我



当时的想法：愿望不代表现实。”这次讲座提出了整个关于抽象黎曼假设的框架。如果这样的语言可以用来适应素数理论，那么演讲者就有可能证明黎曼假设。但是塞尔伯格抱怨说，“他连需要的假设都没有。也许这并不是思考数学的正确方式，他应该从某些可以掌控的结果出发。这次讲座包含了很有趣的内容，但是也是一种趋势的例证，我认为这种趋势很危险。”

301

但是对格罗腾迪克而言这并不是为了抽象而抽象。在他的观点里，这是由数学试图解决的问题所迫使的一场必要的革命，因此他写了一本又一本著作来描述这种新语言。格罗腾迪克的观点是救世主式的，他吸引了一群忠实的信徒。格罗腾迪克的著作非常多，大概有上万页。当一位来访者抱怨研究院图书馆中可怜的藏书时，格罗腾迪克回答道，“我们根本不读这里的书，我们写书。”

哥德尔曾说，在黎曼假设真正被掌握之前，我们必须扩充这门学科的基础。格罗腾迪克革命性的语言就是这种尝试的第一步，然而经过了他的努力，黎曼假设仍然令人失望地在他的可及范围之外。不过格罗腾迪克的革命解决了许多其他问题，包括魏伊提出的关于方程解的个数的重要猜想，但是并不包括黎曼假设。

实际上，格罗腾迪克没能成功地登上黎曼峰，他父亲的政治背景要负起全部责任。格罗腾迪克尽力去实现父亲的政治理想，成为了一名坚定的和平主义者，并参加了20世纪60年代的反军备竞赛运动。他强烈地反对苏联逐渐恶化的政治形势——他是如此的厌恶，以至于在1966年由于在代数几何方面的贡献而被授予菲尔兹奖时，他都拒绝去莫斯科领奖，以抗议前苏联的军事扩张。

由于长期在数学世界中的探索，造成了格罗腾迪克政治上相当单纯的性格。有一次他看到自己将要做主要报告的会议海报，上面写着由NATO① 组织赞助，格罗腾迪克立刻天真地问NATO是一个什么样的组

---

① NATO，全称为North Atlantic Treaty Organization，北大西洋公约组织。



织。当别人告诉他这是一个军事组织的时候，他立即写信给会议组织者以退出相威胁。（最后组织者为了留住他而放弃了这笔赞助。）1967 年，格罗腾迪克在北越南丛林中面对一群目瞪口呆的听众，就抽象代数几何作了一场简短的报告，当时河内大学为躲避轰炸而撤退至此。他把自己全是抽象思想的报告看作是对听力所及范围内的战争的抗议。 302

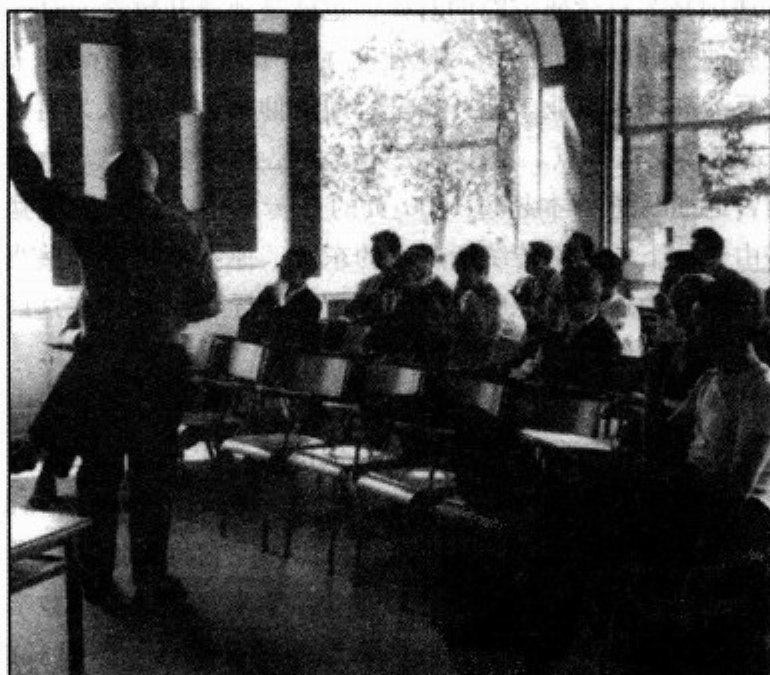
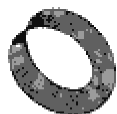


图 46　格罗腾迪克在法国高等科学研究院进行报告

事情在 1970 年发展到顶峰，当格罗腾迪克发现研究院的某些秘密经费是来自军方之后，他直接找到院长雷昂・默尚以辞职相威胁。而研究院成立时的背后力量默尚，并不像数年前的那些会议组织者一样通融，因此格罗腾迪克坚持了自己的原则，离开了研究院。那些与他比较亲近的人认为，他也许是用军事资助作为借口来逃离研究院形成的金色鸟笼。对格罗腾迪克而言他再也不是研究院刚成立时主要的数学成员了，他很高兴能离开这里——他厌倦了长期的舒适状态。当时格罗腾迪



克42岁，关于数学家只能在40岁之前做出最好工作的传言也开始困扰着格罗腾迪克，如果他剩下的数学生涯全无创造性，那情况又将如何？格罗腾迪克不是一个可以活在过去荣耀之上的人。由于在标记位于海平面的点的工作中不能取得任何进展，他逐渐变得清醒：在研究院的舒适环境中，他无法做出比魏伊在监狱中做出的结果更好的东西。当格罗腾迪克离开法国高等科学研究院的时候，也就是他离开数学的时候。

格罗腾迪克开始四处游荡。他建立了一个叫做“幸存者”的组织，用来处理反战和环保事业。他开始全心地信仰佛教，并认为自己的哈西德派[①]祖先能接受这一点。由于无法完成自己的数学设想，他把这些感受到的痛苦通通写进一本超过1000页的自传之中，在其中他猛烈地攻击了那些由他留下的数学传统所产生的东西。他不能接受那些当年的追随者现在已经成为这场由他所开创的革命的领导者，并且在这门科学中留下他们各自的印记。

303

在离开研究院30年之后，现在格罗腾迪克住在比利牛斯山脉附近的偏远小村子里。据一些几年前拜访过他的数学家说，“他正因为恶魔而困扰，他觉得在世界各地都有恶魔的存在，破坏了神圣的和谐。”格罗腾迪克认为恶魔应该对一些事情负责，比如说它将光速从优美的整值300 000千米每秒改变为“丑陋的”299 887千米每秒。如果数学家能够像在家里一般畅游整个数学世界，那么他们都必须有一些疯狂的性格。格罗腾迪克在探索数学世界之外的世界所花费的时间让他无法找到回家的路。

格罗腾迪克并非唯一的因为试图证明黎曼假设而发疯的数学家。在20世纪50年代后期，约翰·福布斯·纳什（John Forbes Nash）在早期的成功之后，也被证明黎曼假设的愿望所迷住。据西尔维亚·娜萨（Sylvia Nasar）在纳什的自传《美丽心灵》中所述，人们都在“议论纳什爱上了科恩”，一位同样研究黎曼假设的人。纳什向保罗·科恩谈论

---

① 犹太教的一个派别，出现于基督教兴起之前，起源不详，又称为虔敬派。



自己的大量思想，但是科恩预料到这并不会有什么结果。有人相信由于科恩对纳什的拒绝——既有感情上的也有数学上的——使得纳什脆弱的心灵最终崩溃。1959年，纳什被邀请在纽约哥伦比亚大学美国数学会的会议上介绍自己的想法。事实证明这是一场灾难，纳什在众多听众面前失去了理智，不停地给出无意义的论断宣称自己已经证明了黎曼假设，听众则目瞪口呆地坐在下面。格罗腾迪克和纳什正体现了沉迷于数学的危险。（和格罗腾迪克不同，纳什最后从疯狂的边缘恢复正常，并由于自己发展了博弈理论的数学而获得1994年的诺贝尔经济学奖。）

相比较于格罗腾迪克经历的精神崩溃，他的数学结构仍然矗立。不少人认为我们仍然缺乏的关键思想将会扩充格罗腾迪克的革命，并最终解开素数的秘密。到了20世纪90年代中期，数学界又因为格罗腾迪克的继任者即将到来而兴奋起来。

304

最后的笑声

当阿兰·科纳打算做黎曼假设的传言开始流传时，许多人扬起了眉毛。作为法国高等科学研究院和法兰西学院的教授，科纳是一位在名声上可以匹配格罗腾迪克的重量级人物。他发明的非交换几何实际上就是魏伊和格罗腾迪克几何的推广。和格罗腾迪克一样，在其他人只能看到混乱表面的时候，科纳能够看到其中的内部结构。

在数学中，“非交换”意味着你在做某些事情时顺序是至关重要的。比如说，取某人面部的方形照片正面朝下放置。首先，将照片从右向左翻转，并沿顺时针方向旋转90°。然后重复这个实验，只不过是先旋转再翻转（在此注意翻转的方向仍然是从右向左），这时你会发现面部正好朝着相反的方向，此时结果就依赖于你先做哪一步操作。同样的原理也存在于量子物理的许多神秘性之内，海森伯的不确定性原理告诉我们永远无法准确知道一个粒子的位置和它的动量。这种不确定性的数学原因就在于你是先测量位置还是先测量动量。

在某些不存在对称性的数学区域中，科纳引入了魏伊和格罗腾迪克的几何，揭示了一个全新的数学世界。而在同时期，大部分数学家正在为了更好地理解那些可见的数学世界而花费精力。每隔数代人就会出现一位探索者，他能冲破原有的界限，发现未知的新大陆，科纳就是这样的探索者。

对科纳而言这些探索源于非常强烈的感情。他对于数学的热爱可以追溯到他7岁时初次尝试解决基本数学问题的时候。“我非常清楚地记得当我沉浸到那种聚精会神的特殊状态时所感受到的强烈的愉快感觉，这是做数学所必须的。”看上去他再也没有脱离这种沉醉的状态，并且面对所有可怕的理论和抽象概念，科纳仍保留了某些他在7岁时所拥有的孩子气般的顽皮。对科纳而言，数学是最能带你靠近终极真理的科学，远胜于其他科学，并且充满乐趣的追寻过程也是让他从童年时代就献身这门科学的部分原因。他这样描述数学，因为“数学实在不受时空的限制，它能提供——当你足够幸运地发现哪怕是最微小的一部分之后——由数学的不朽性带来的一种非常愉悦的感受”。

305

科纳认为数学家就是那种永远有活力、永远在搜寻新大陆的人。当其他人只愿意在已知的海岸附近航行时，科纳更愿意抛开熟悉的数学领域，向着位于我们目前数学地平线之外的未知水域进发。他能发现素数与非交换几何抽象世界之间的联系这一事实，应该归功于他能将旅行中碰到的不同数学文化综合起来的能力。有些数学家喜欢两人或多人合作搞研究，他们的能力合在一起可以帮助他们穿越数学的海洋，而单凭个人的力量也许会失败。但是科纳则是那种沉迷于孤独的旅行者，“如果一个人真的希望发现什么的话，最好还是一个人。”

科纳发现的新几何由魏伊和格罗腾迪克发展的代数几何推广而来。魏伊和格罗腾迪克提供给我们的是一本新字典，它可以用来将几何翻译为代数。这本字典的功用体现在，如果一个问题在几何语言的表述下是模糊不清、充满神秘的，那么当它被翻译成代数语言之后就变得显而易见。这就是魏伊如何解决方程解的个数问题的方法、以及证明另外一些



函数空间中零点都落在同一直线上时所用的方法。如果单单试图理解这些方程所描述的几何形状，魏伊根本无从下手，但是一旦他利用了自己的代数-几何字典之后，他就有方法来理解这些问题了。

魏伊的几何回答了纯数论中的问题，而科纳的思想则为超弦理论学家和量子物理学家急切希望建立的几何提供了一种数学描述。在20世纪末期，物理学家迫切需要一种新的几何理论支持超弦理论，超弦理论是在70年代引进的用于处理量子物理和相对论之间不相容问题的一种可能的答案。科纳对此产生了兴趣，开始寻找物理学家认为应该存在的这种几何。科纳知道，对于这种几何，即使没有物理部分的清晰事实，他仍然可以建立抽象的代数部分。这个发现只有那些熟悉抽象数学的人才能建立——凭物理直觉是远远不够的。

亚原子世界的奇怪行为迫使科纳抛开那些用来理解常规几何的标准方法。如果说黎曼的几何革命为爱因斯坦提供了描述巨大范围物理学的语言，那么科纳的几何就为数学家提供了了解极小世界中奇怪几何的机会。多亏了科纳，我们才有可能解读空间的微细结构。

306

休·蒙哥马利和麦克尔·贝里已经发现了素数和量子混沌之间可能的联系，而科纳的发现是适合量子物理的完美语言。这一事实让越来越多的人对他进攻黎曼假设这件事持乐观态度。再加上他是来自于法国数学复兴时期，在这一时期已经有一些新的技巧可以用来探索 ζ 函数空间，因此数学界都开始相信也许结果即将到来。最终所有的线索都将汇聚到一起。

科纳发现的东西是一个非常复杂的构建于代数世界上的几何空间，称为赋值矢量类上的非交换空间。为了构造这个空间科纳利用了在20世纪初发现的一种奇怪的数，称为 p 进制数（p-adic number）。对每个素数 p，总存在着一类 p 进制数。科纳认为将这些数粘合在一起，然后观察在这种高度奇异空间中的乘法作用，那么在这个空间中黎曼零点就会自然地显现出共鸣。他的方法像非常奇怪的混合了多种成分的鸡尾酒，这些成分来自于数世纪对素数的研究。因此一点也不奇怪为什么数学家



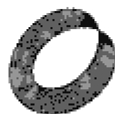
会对他的成功充满了希望。

科纳并非一位专横的数学家，但却是一位有魅力的表演者。许多人都被他关于黎曼假设的演讲迷住。我也听过他的报告，并深信从他描述的工作出发，最终将得到黎曼假设的证明，并且他已经做完了所有困难的部分，剩下的就是有人能添上最后一笔。虽然这是许多人期望拥有的伟大思想，但是科纳自己知道仍然有许多部分需要填补。“验证的过程往往会十分痛苦，人们十分害怕犯错误……它包含了大量的焦虑，因为某人不可能知道自己的直觉是否正确——这和做梦差不多，在那里直觉经常被证明是错误的。”

在1997年春天，科纳来到普林斯顿向一些大人物介绍自己的思想：邦比艾里、塞尔伯格和萨那克。除了巴黎希望夺回自己的优势，普林斯顿仍然是无可置疑的黎曼假设的麦加圣地。塞尔伯格已经成为这个问题的教父——在通过这样一位与素数战斗超过半个世纪的人的审查之前，任何结果都不符合要求。萨那克则是年轻一代的代表，他像剑一般的思想可以刺中任何最微小的缺陷。最近另外一位同样来自普林斯顿的尼克·卡兹（Nick Katz）加入了萨那克的队伍，卡兹是魏伊和格罗腾迪克发展的新数学领域毫无疑问的大师。他们两人一起证明了我们认为是描述黎曼世界中零点的随机鼓的奇怪统计量，可以用魏伊和格罗腾迪克考虑的函数世界明确地表示出来。卡兹的眼光非常锐利，几乎没有什么错误能逃脱他的注视，数年前，正是卡兹发现了怀尔斯关于费马大定理不正确的第一版证明中的错误。

307

邦比艾里作为了解黎曼假设的大师郑重地坐在最后。他曾因为给出到目前为止真实素数个数和高斯估计之间的误差的最好结果而得到菲尔兹奖，这一证明有时也被数学家称为“平均意义上的黎曼假设”。在他可以俯瞰环绕研究院森林的安静的办公室里，邦比艾里集结了多年来所有的想法准备向最完整的答案发动最后的攻击。和卡兹一样，邦比艾里同样有一对锐利的双眼。作为一名集邮爱好者，邦比艾里曾得到一次购买一张非常稀有邮票的机会，以充实自己的收藏。但是经过仔细观察，



他发现了三处瑕疵。于是他将邮票还给卖家，并指出了其中两处瑕疵，第三处微小的瑕疵他记在了心里——便于在未来的日子里分辨出改良的赝品。任何有希望的黎曼假设的证明都必须接受如此细心的检查。

塞尔伯格、萨那克、卡兹和邦比艾里，这是令人敬畏的出场阵容，但是科纳一点也没有胆怯。他论证中的力量和他的个性与这些普林斯顿的权威相比并不差多少。科纳知道自己虽然还没有任何证明，但是他确信自己的观点是到目前为止最好的解决黎曼假设的途径。这个方法融合了从量子物理到包含魏伊和格罗腾迪克的数学直觉在内的许多思想。

普林斯顿的大师们承认科纳确实取得了一些进展，但是他们也能看出问题依然没有得到解决。萨那克看出科纳成功地发展了一套思想，这是在他到达斯坦福不久就听自己的导师保罗·科恩说过的思想。两者的差别在于，科纳拥有一套复杂的新语言和新技巧，让科恩的思想变得更加明确。但是在科纳的方法中仍然存在一个问题：看上去他对所有的东西进行了重新安排，使得那些应该落在黎曼临界线之外的点变得不可见了。就像一个魔术师，科纳只让你看见那些落在临界线上的点，而那些落在临界线之外的点都消失在他的数学衣袖中。

308

"科纳让观众都陷入迷糊，"萨那克说，"他真是一个有说服力的人，并且充满魅力。如果你指出他方法中的一个难点，下一次他看到你时就会说，'你说的很正确。'这就是他如何轻易地收买人心的关键。"萨那克解释说，在当时科纳快速地介绍了证明中下一个新的方法。萨那克相信科纳仍然缺少某种魔力，那种让魏伊在1940年的监狱中做出突破的魔力。邦比艾里也表示了同意，"我仍然认为缺乏一些主要的新思想。"

在科纳的报告之后不久，邦比艾里收到一封来自好朋友、坦普尔大学（University of Temple）的多荣·蔡尔博格（Doron Zeilberger）的电子邮件，在其中他声称发现了 π 的最令人惊奇的性质。但是聪明的邦比艾里很快就看到邮件的日期：四月一日。为了表明自己已经收到这个玩笑，邦比艾里用同样的方式回了一封信。他将科纳关于找到素数规律的



事情以恶作剧方式融合到了信件中："阿兰·科纳上周三于高等研究院所作的报告中提到了一些有趣的进展……"观众中的一位年轻物理学家立刻明白了如何完成科纳的计划。黎曼假设是正确的。"请尽可能广泛地转发此消息。"

蔡尔博格帮了邦比艾里的忙，一周之后这条通知出现在了即将到来的国际数学家大会的网站的电子公告牌上，以供全世界数学家阅读。邦比艾里激起的兴奋之火需要一段时间才能扑灭。当科纳回到巴黎，发现别人都在讨论这条新闻。尽管这个玩笑是针对那位物理学家，科纳仍然显得十分沮丧。

邦比艾里的愚人节玩笑看起来标志着科纳关于黎曼假设工作所带来的兴奋感的结束。现在一切归于平静，似乎科纳的想法能解开素数秘密的希望也随之破灭。即使在科纳复杂的非交换几何世界中，素数也是难以捉摸的。在科纳涉及该问题之后几年，黎曼的城堡仍然大门紧闭。当然，科纳的方法仍有可能奏效，只是在此之前有许多工作要做，不过他认为能轻松获得证明的意识已经消失不见。守护黎曼假设的城墙现在看上去也许有了些许的不同，但是仍和从前一样无法攻破。

309

科纳面对这个僵局倒是显得泰然自若。当百万美元寻求黎曼假设解答的消息被公布之后，他说，"对我而言，数学一直是学习谦卑的最好学校。数学主要的价值就体现在数学之中存在着无限的困难问题，就像喜马拉雅山一样，到达顶峰是一件极其困难的事，因此我们不得不付出代价。但是问题在于，一旦我们到达了顶峰，那里的风景将极其美妙。"科纳并没有放弃他的追求，他仍然继续作战，希望能发现最后的重要思想从而完成征途。他渴望那种奇妙的时刻，那种出现在每个数学家生命中的灵感时刻。"灵感出现的瞬间，会占据你全部的情感，你不可能保持被动或是不在意。当我真正体验那种罕见瞬间的时候，我甚至不能抑制眼中流下的泪水。"

因此，我们不得不继续倾听神秘的素数节奏：2，3，5，7，11，13，17，19，…素数随着数的宇宙不断向远方延伸，永远也不会枯竭。



它们是数学的中心，是构成后续所有元素的基石。抛开我们追求规律和解释的愿望，我们是否真的不得不接受这个事实，即这些基本的素数也许永远在我们的能力范围之外？

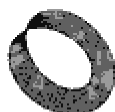
欧几里得证明了素数总是一个接一个。高斯猜测素数就像扔硬币一样是随机决定的。黎曼则通过虫洞被吸入一个虚数世界，在其中素数转化为音乐。在这个世界中，每个位于海平面的点发出一个音符。人们的探索就是希望能够读懂黎曼的藏宝图，找到每个位于海平面的点的位置。利用没有公布于众的秘密公式，黎曼发现尽管素数是无序的，但是在他的世界中的零点却是有规律的，它们整齐地排列在一条直线上而非随机地散布于各处。黎曼无法在自己的世界中看得更远，判断这样的规律是否永远正确，但是他相信这是正确的，因此就出现了黎曼假设。

如果黎曼假设正确，那么不存在某个音符的声音比其他的都要响；演奏素数音乐的这个乐队将会处于完美的平衡状态。它也能解释为什么我们在素数之中找不到比较明显的规律，因为明显的规律就代表着某件乐器的声音盖过其他乐器，但是由于乐器被完美地组合在一起，规律本身也就相互抵消，留下的就是素数毫无规律的消长。

如果黎曼假设正确，它就能帮我们理解为什么素数看上去好像是由掷硬币决定的。但也许黎曼关于这些海平面上的点的直觉只是他的如意算盘而已；也许随着音乐的发展，素数乐队中某件特殊的乐器开始统治整首歌曲；也许在数的极远之处会发现某种规律；也许当大自然一遍又一遍地抛出素数硬币决定我们居住的这个数学宇宙时，硬币会开始出现偏差。正如我们已经了解的那样，素数也许是一群带有恶意的小东西，将它们真正的本色隐藏于外表之下。

310

因此随之开始了一场证实黎曼信念的征途，来证实黎曼的素数藏宝图上的点都位于同一直线。我们已经游历了数学历史和物理世界：拿破仑革命时期的法国；德国的新人文主义革命，从柏林到中世纪小镇哥廷根；剑桥和印度的奇怪联盟；战火中被孤立的挪威；在新世界的普林斯顿，新成立的研究院接纳了那些饱受战火蹂躏而逃离欧洲的黎曼圣杯的



勇敢追寻者；最后是现代的巴黎以及一种新语言，这种语言最初来自于监狱的小牢房中，并让一位主要发展者因此精神错乱。

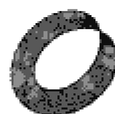
素数的故事也开始流传到了数学世界之外，技术的发展改变了我们做数学的方式。诞生于布莱切利庄园的计算机，为我们提供了观察到那些曾经处于我们观察范围之外的数的能力；量子物理的语言使得数学家可以清楚地发现那些在科学文化交融之前从未观察到的规律和联系；甚至是像 AT&T、惠普以及加州的电器商店这样的商业企业也成为故事中的一员。素数在计算机安全方面的中心地位也让这些数出现在聚光灯之下，现在素数影响着我们所有人的生活，保护着世界的电子秘密不被网络黑客窃取。

抛开这些迂回曲折，素数依然难以捉摸。每次我们将它们赶到一个新的领域，像科纳的非交换世界或是贝里的量子混沌领域，它们总是能找到一个新的藏身之处。

许多为我们理解素数做出贡献的数学家都得到了长寿的回报。由于在 1896 年证明了素数定理，雅格斯·哈达马和查尔斯·德·拉·瓦勒普桑都活到了 90 多岁。人们开始相信正是因为他们证明了素数定理才使得他们如此长寿。相信长寿与素数之间存在联系的观点同样被阿特勒·塞尔伯格和保罗·厄多斯证实，他们由于在 20 世纪 40 年代给出了素数定理的初等证明而活到了 80 多岁。数学家开玩笑地提出一个新的猜想：证明了黎曼假设的人将获得永生。另外一个笑话是，在某处某人已经推翻了黎曼假设，不过没有人听说过，因此这位不幸的数学家当时就魂飞西天。

311

关于我们离结果还有多远这个问题，存在着多种观点。曾经计算过黎曼藏宝图中海平面上大量点的安德鲁·奥德兹克相信我们无法预测这个时间，“也许就在下一周，也许是一个世纪之后，这个问题看起来非常困难。我怀疑它是否就是某种非常简单的东西，只是由于如此多的大师花去如此长的时间和如此多的精力来研究它。但是很可能下周就会有某人想出一个绝妙的主意。”其他人估计我们在解决这个问题之前还需



要至少两个重要的想法。

休·蒙哥马利相信，在由他和量子物理学家弗里曼·戴森在普林斯顿茶会上的交谈引出的结果出现之后，我们已经在攀登黎曼高峰的过程中完成了相当一部分的路程。但是他也为自己的乐观加上了清醒的注解："我们已经有了黎曼假设的证明，只不过其中还存在着一段缺陷。不幸的是，这个缺陷恰好位于问题的开始。"正如蒙哥马利指出的那样，这个缺陷出现的不是地方。任何缺陷都是致命的，位于中间的缺陷至少意味着我们在旅程中已经有了进展；但是位于路程开始的缺陷则意味着除非我们能找到一条穿过第一道关卡的道路，否则我们发现的那些通往黎曼高峰的路程都是无用的。"这造成了理论中的一个僵局，而我们不能证明这第一个定理。"

尽管有100万美元的刺激，许多数学家仍然不太敢靠近这个声名显赫的难题。因为许多伟大的名字都尝试过并且失败了：黎曼、希尔伯特、哈代、塞尔伯格、科纳等等……但是仍然有一些勇士愿意尝试，也许我们能在将来看见他们的名字，其中有德国的克里斯托夫·德宁格（Christopher Deninger）和以色列的夏伊·哈让（Shai Haran）。

许多人预测黎曼假设将会安全度过它的200周年。有人认为它的末日已经快要到来，因为有了如此多的证据告诉我们该到何处去寻找答案，它不可能持续那么长时间不被解决。有人认为它的命运落在哥德尔的手中：最终它将被证实是正确的，但是不可证明。有人相信他们已经证明了黎曼假设，只是数学权威机构不敢承认这一点。当然还有一些人在寻找答案的过程中走上了疯狂之路。

也许我们太注重于通过高斯和黎曼的观点来观察素数，以至于我们失去了某种简单地理解这些谜一样数字的不同方法。高斯给出了素数个数的估计；黎曼预测这个估计在最坏的情况下与真实值相差 N 的平方根；利特伍德证明了你无法做得比这个结果更好。也许存在着另外一个观察角度，只是由于我们太过于关注高斯建造的一切，以至于没有人注意这一点。

312



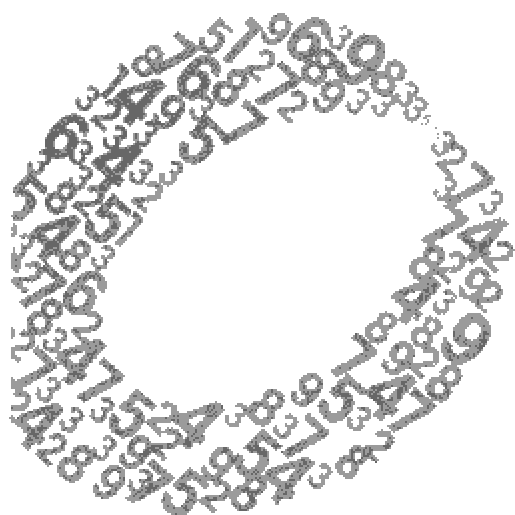
和谋杀推理案件中的主角一样，我们也在不断地审视那些数学嫌疑犯。是谁或者是什么东西让这些零点全部落在黎曼临界线上？案件中疑点遍布，到处都是指纹，我们也有了结果的画像——然而我们依然抓不住答案。不过令人安慰的是，即使素数永远也不暴露它们的秘密，它们仍然会带领我们在最不平凡的智力征途上前进。它们拥有的重要性已经远远超过它们原先作为算术原子的基本功能。就像我们已经发现的，迄今为止素数已经为我们打开了数学中看上去毫无联系的领域之间的大门，数论、几何、分析、逻辑、概率论、量子物理——所有的这些都在我们追寻黎曼假设的过程中被联系起来。这样的过程将数学置于一种新的观点之下，我们惊喜地发现数学中存在着千丝万缕的相互联系：数学从一门寻找规律的学科转变成一门寻找联系的学科。

这样的联系不仅仅存在于数学世界之中。素数曾被认为是最抽象的概念，在学术的象牙塔之外没有任何重要性可言。以哈代为代表的数学家曾经很享受能够研究这种孤立的、不受外部世界影响的对象。但是素数再也不会为数学家提供一个逃避真实世界压力的出口，就像它曾为黎曼和其他人做过的那样。现在，素数是现代电子世界安全性的关键，它们和量子物理的共振也许还能告诉我们它们具有某些物理世界的本性。

即使我们成功地证明了黎曼假设，仍然有更多的问题和猜想在急切地等着我们。许多新的有趣的数学内容正等待着黎曼假设的解决，从而可以得到进一步的发展。结果只是一个开始，是打开一片全新处女地的开始。用安德鲁·怀尔斯的话来讲，黎曼假设的证明为我们提供了探索新世界的可能性，在历史上，经度问题的解决使得18世纪的探险家能够探索真实的新世界。

在那一天到来之前，我们还将继续倾听这首不可预测的数学音乐，而无法掌握它的转承起合。素数曾经是我们探索数学世界的长期伙伴，然而它们仍将是最高深莫测的数。抛开那些伟大数学思想为了解释这首神秘音乐的韵律和变换作出的努力，素数仍然是一个未解之谜。我们还将等待某人的出现，他的名字将随着素数的音乐而流芳百世。

313
314



致 谢

我的许多同事都慷慨地奉献出他们的时间和对我的支持。我要特别感谢以下几位，感谢他们乐意坐下来和我谈论他们的观点和看法：Leonard Adleman，Sir Michael Berry，Bryan Birch，Enrico Bombieri，Richard Brent，Paula Cohen，Brian Conrey，Persi Diaconis，Gerhard Frey，Timothy Gowers，Fritz Grunewald，Shai Haran，Hendrik Lenstra，Alfred Menezes，Hugh Montgomery，Andrew Odlyzko，Samuel Patterson，Ron Rivest，Zeev Rudnick，Peter Sarnak，Dan Segal，Atle Selberg，Peter Shor，Herman te Riele，Scott Vanstone 和 Don Zagier.

我要特别感谢麦克尔·贝里爵士。我们初次相识于唐宁街10号的楼梯上，当时我们正在排队等待和首相握手。贝里爵士让我注意到了素数中包含的音乐，本书的书名正是来源于那次相遇的启发。

对那些认真阅读了本书部分或全部草稿的人们，我也要向他们表示感谢：Sir Michael Berry，Jeremy Butterfield，

Bernard du Sautoy，Jeremy Gray，Fritz Grunewald，Roger Heath-Brown，Andrew Hodges，Jon Keating，Angus Macintyre，Dan Segal，Jim Semple and Eric Weinstein。本书中如有任何错误则由我本人负责。

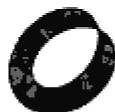
还有许多书籍、论文和文章为本书提供了无价的背景资料，其中大部分列在了"进一步的阅读材料"中，我特别要指出的是 *Notices of the American Mathematical Society* 杂志，它上面一直源源不断地出现许多关于数学和数学界的好文章。

许多机构在我写这本书的过程中也给予了帮助，包括美国数学研究院，Certicom，哥廷根大学图书馆，佛洛汉庄园的 AT&T 实验室，普林斯顿高等研究院，布里斯托的惠普实验室和波恩的马克思·普朗克数学研究所。

对那些帮助这本书面世的出版界朋友，我非常高兴能在此表达我对他们的谢意：我的代理人，Greene & Heaton 代理公司的 Antony Topping，他在本书从萌芽到出版的整个过程中一直提供了帮助；Judith Murray 将我们联系到一起；我的书籍编辑，Fourth Estate 公司的 Christopher Potter、Leo Hollis 和 Mitzi Angel 以及 HarperCollins 公司的 Tim Duggan；我的稿件编辑 John Woodruff。我要特别感谢 Leo，他花了很长时间研究四维空间。

如果没有皇家学会的支持我将没有机会进行这本书的写作。作为皇家学会的研究成员，我不光有机会追逐我的数学梦想，同时还可以表达自己这一路体验到的兴奋。皇家学会不仅仅代表着一个银行账户——他们也关心那些受到资助的人。他们支持将数学传播给大众的行为本身就是无法估价的。

我还要感谢一些在媒体工作的朋友，他们冒着风险公布并帮助宣传我的第一份关于严肃数学的作品，还有那些耗费时间帮助我写作的朋友：泰晤士报的 Graham Patterson，Philippa Ingram 以及 Anjana Ahuja；BBC 的 John Watkins 和 Peter Evans；Science Spectra 的 Gerhart Friedlander。另外我还要感谢 NCR 和 Milestone 提供的机会，让我可以为银行界

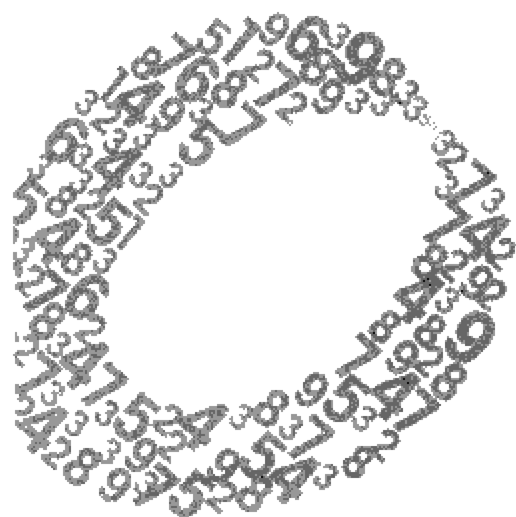


人事讲解数学。

我能成为一名数学家，多亏了中学时期的一位老师拜尔森先生（Mr. Bailson），是他首次在教室中向我展示了算术中的音乐。除了他之外，还有Gillotts综合中学、King James's 6th Form College、Wadham College、Oxford都给了我不同寻常的教育。

当我写这本书的时候，还要感谢阿森纳队获得的双料冠军。海伯利球场为我提供了一个极佳的地点，让我释放出与黎曼角力之后的压力。

作为个人的注记，我在这里要感谢我的朋友和家庭的帮助：我的父亲，他帮助我了解到数的魔力；我的母亲，她帮助我了解到语言的魔力；我的祖父母，特别是彼得，他是我的动力；我的爱人莎妮，感谢你的耐心和坚信我能写好这本书的信心。我最大的感谢要留给我的儿子托默，感谢他在我工作一天之后的陪伴，没有他我就没法坚持完成这本书。



进一步的阅读材料

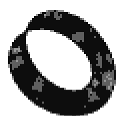
下面的许多书籍和文章为撰写本书提供了重要的材料。对那些由于读了本书而希望了解该学科更深内容的读者，我推荐你们参看下面这个目录。在此目录中除了一些包括了某些有趣的非专业观点的材料之外，我没有选择那些包含高度专业、需要数学学位才能读懂的材料。

Albers, D. J., Interview with Persi Diaconis, *in Mathematical People: Profiles and Interviews*, ed. D. J. Albers and G. L. Alexanderson (Boston: Birkhäuser, 1985), pp. 66~79

Aldous, D., and Dianconis, P., 'Longest increasing subsequences: from patience sorting to the Baik-Deift-Johansson theorem', *Bulletin of the American Mathematical Society*, vol. 36, no. 4 (1999), pp. 413~432

Alexanderson, G. L., Interview with Paul Erdös, in *Mathematical People: Profiles and Interviews*, ed. D. J. Albers and G. L. Alexanderson (Boston: Birkhäuser, 1985), pp. 82~91

Babai, L., Pomerance, C., and Vértesi, P., 'The Mathematics of Paul Erdös', *Notices of the American Mathematical Society*,



vol. 45, no. 1 (1998), pp. 19 ~ 31

Babai, L., and Spencer, J., 'Paul Erdös (1913 ~ 1996)', *Notices of the American Mathematical Society*, vol. 45, no. 1 (1998), pp. 64 ~ 73

Barner, K., 'Paul Wolfskehl and the Wolfskehl Prize', *Notices of the American Mathematical Society*, vol. 44, no. 10 (1997), pp. 1294 ~ 1303

Beiler, A. H., *Recreations in the Theory of Numbers: The Queen of Mathematics Entertains* (New York: Dover Publication, 1964)

Bell, E. T., *Men of Mathematics* (New York: Simon & Schuster, 1937)

Berndt, B. C., and Rankin, R. A. (eds), *Ramanujan: Letters and Commentary*, History of Mathematics, vol. 9 (Providence, RI: American Mathematical Society, 1995)

Berndt, B. C., and Rankin, R. A. (eds), Ramanujan: Essays And Surveys, History of Mathematics, vol. 22 (Providence, RI: American Mathematical Society, 2001)

Berry, M., 'Quantum physics on the edge of chaos', *New Scientist*, *November* 19 (1987), pp. 44 ~ 47

Bollobás, B. (ed.), *Littlewood' s Miscellany* (Cambridge: Cambridge University Press, 1986)

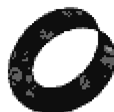
Bombieri, E., 'Prime territory: exploring the infinite landscape at the base of the number system', *The Sciences*, vol. 32, no. 5 (1992), pp. 30 ~ 36

Borel, A., 'Twenty-five years with Nicolas Bourbaki, 1949 ~ 1973', *Notices of the American Mathematical Society*, vol. 44, no. 3 (1998), pp. 373 ~ 380

Borel, A., Cartier, P., Chandrasekharan, K., Chern, S. -S., and Iyanaga, S., 'André Weil (1906 ~ 1998)' *Notices of the American Mathematical Society*, vol. 46, no. 4 (1999), pp. 440 ~ 447

Bourbaki, N., *Elements of the History of Mathematics*, translated from the 1984 French original by John Meldrum (Berlin: Springer-Verlag, 1994)

Breuilly, J. (ed.), *Nineteenth-Century Germany: Politics, Culture and Society* 1780 – 1918 (London: Arnold, 2001)



Calaprice, A. (ed.), *The Expanded Quotable Einstein* (Princeton, NJ: Princeton University Press, 2000)

Calinger, R., 'Leonhard Euler: the first St. Petersburg years (1727 ~ 1741)', *Historia Mathematica*, vol. 23, no. 2 (1996), pp. 121 ~ 166

Campbell, D. M., and Higgins, J. C. (eds), *Mathematics: People, Problems, Results*, 2 vols (Belmont, CA: Wadsworth International, 1984) [其中包括了有关布尔巴基、高斯、利特伍德、哈代、哈瑟、剑桥数学、希尔伯特及其问题、证明的本质和哥德尔定理等内容]

Cartan, H., 'André Weil: memories of a long friendship', *Notices of the American Mathematical Society*, vol. 46, no. 6 (1999), pp. 633 ~ 636

Cartier, P., 'A mad day' s work: from Grothendieck to Connes and Kontsevich. The evolution of concepts of space and symmetry', *Bulletin of the American Mathematical Society*, vol. 38, no. 4 (2001), pp. 389 ~ 408

Changeux, J.-P., and Connes, A., *Conversations on Mind, Matter, and Mathematics*, edited and translated from the 1989 French original by M. B. DeBevoise (Princeton, NJ: Princeton University Press, 1995)

Connes, A., Lichnerowicz, A., and Schützenberger, M. P., *Triangles of Thoughts*, translated from the 2000 French original by Jennifer Gage (Providence, RI: American Mathematical Society, 2001)

Connes, A., 'Noncommutative geometry and the Riemann zeta function', in *Mathematics: Frontiers and Perspectives*, edited by V. Arnold, M. Atiyah, P. Lax and B. Mazur (Providence, RI: American Mathematical Society, 2000), pp. 35 ~ 54

Courant, R., 'Reminiscences from Hilbert' s Göttingen', *The Mathematical Intelligencer*, vol. 3, no. 4 (1981), pp. 154 ~ 164

Davenport, H., 'Reminiscences of conversations with Carl Ludwig Siegel. Edited by Mrs Harold Davenport', *The Mathematical Intelligencer*, vol. 7, no. 2 (1985), pp. 76 ~ 79

Davis, M., *The Universal Computer: The Road from Leibniz to Turing*, (New York, NY: W. W. Norton, 2000)



Davis, M., 'Book review: *Logical Dilemmas: The Life and Work of Kurt Gödel and Gödel: A Life of Logic*', *Notices of the American Mathematical Society*, vol. 48, no. 8 (2001), pp. 807 ~ 813

Dyson, F., 'A walk through Ramanujan' s garden', in *Ramanujan Revisited*, edited by G. E. Andrews, R. A. Askey, B. C. Berndt, K. G. Ramanathan and R. A. Rankin (Boston, MA: Academic Press, 1988), pp. 7 ~ 28

Edwards, H. M. *Riemann' s Zeta Function*, Pure and Applied Mathematics, vol. 58 (New York, NY: Academic Press, 1974) [其中包括了黎曼著名的关于素数的十页论文 'Über die Anzahl der Primzahlen unter einer gegebenen Grösse' 的英文翻译作为附录]

Flannery, S., with Flannery D., *In Code: A Mathematical Journey* (London: Profile Books, 2000)

Gardner, J. H., and Wilson, R. J., 'Thomas Archer Hirst - Mathematician Xtravagant III. Göttingen and Berlin', *American Mathematical Monthly*, vol. 100, no. 7 (1993), pp. 619 ~ 625

Goldstein, L. J., 'A history of the prime number theorem', *American Mathematical Monthly*, vol. 80, no. 6 (1973), pp. 599 ~ 615

Gray, J. J., 'Mathematics in Cambridge and beyond', in *Cambridge Minds*, ed. R. Mason (Cambridge: Cambridge University Press, 1994), pp. 86 ~ 99

Gray. J. J., *The Hilbert Challenge* (Oxford: Oxford University Press, 2000)

Hardy, G. H., 'Mr S. Ramanujan' s mathematical work in England', *Journal of the Indian Mathematical Society*, vol. 9 (1917), pp. 30 ~ 45

Hardy, G. H., 'Obituary notice: S. Ramanujan', *Proceedings of the London Mathematical Society*, vol. 19 (1921), pp. xl ~ lviii

Hardy, G. H., 'The theory of numbers', *Nature*, September 16 (1922), pp. 381 ~ 385

Hardy, G. H., 'The case against the Mathematical Tripos', *Mathematical Gazette*, vol. 13 (1926), pp. 61 ~ 67

Hardy, G. H., 'An introduction to the theory of numbers', *Bulletin of the A-*



merican Mathematical Society, vol. 35 (1929), pp. 778 ~ 818

Hardy, G. H., 'Mathematical Proof', *Mind*, vol. 38 (1929), pp. 1 ~ 25

Hardy, G. H., 'The Indian mathematician Ramanujan', *American Mathematical Monthly*, vol. 44, no. 3 (1937), pp. 137 ~ 155

Hardy, G. H., 'Obituary notice: E. Landau', *Journal of the London Mathematical Society*, vol. 13 (1938), pp. 302 ~ 310

Hardy, G. H., *A Mathematician' s Apology*, (Cambridge: Cambridge University Press, 1940)

Hardy, G. H., *Ramanujan. Twelve Lectures on Subjects Suggested by His Life and Work*, (Cambridge: Cambridge University Press, 1940)

Hodges, A., *Alan Turing: The Enigma* (New York, NY: Simon & Shuster, 1983)

Hoffman, P., *The Man Who Loved Only Numbers. The Story of Paul Erdös and the Search for Mathematical Truth*, (London: Fourth Estate, 1998)

Jackson, A., 'The IHÉS at forty', *Notices of the American Mathematical Society*, vol. 46, no. 3 (1999), pp. 329 ~ 337

Jackson, A., 'Million-dollar mathematics prizes announced', *Notices of the American Mathematical Society*, vol. 46, no. 8 (2000), PP. 877 ~ 879

Jackson, A., 'Interview with Henri Cartan', *Notices of the American Mathematical Society*, vol. 46, no. 7 (1999), pp. 782 ~ 788

Kanigel, R., *The Man Who Knew Infinity: A Life of the Genius Ramanujan*, (New York, NY: Scribner' s, 1991)

Koblitz, N., 'Mathematics under hardship conditions in the Third World', *Notices of the American Mathematical Society*, vol. 38, no. 9 (1991), pp. 1123 ~ 1128

Knapp, A. W., 'André Weil: a prologue', *Notices of the American Mathematical Society*, vol. 46, no. 4 (1999), pp. 434 ~ 439

Lang, S., 'Mordell' s review, Siegel' s letter to Mordell, Diophantine geometry, and 20th century mathematics', *Notices of the American Mathematical Society*,

vol. 42, no. 3 (1995), pp. 339 ~ 350

Laugwitz, D., *Bernhard Riemann, 1826 ~ 1866: Turning Points in the Conception of Mathematics*, translated from the 1996 German original by Abe Schenitzer (Boston, MA: Birkhäuser, 1999)

Lesniewski, A., 'Noncommutative geometry', *Notices of the American Mathematical Society*, vol. 44, no. 7 (1997), pp. 800 ~ 805

Littlewood, J. E., *A Mathematician's Miscellany* (London: Methuen, 1953)

Littlewood, J. E., 'The Riemann hypothesis', in *The Scientist Speculates: An Anthology of Partly-Baked Ideas*, edited by I. J. Good, A. J. Mayne and J. Maynard Smith (London: Heinemann, 1962), pp. 390 ~ 391

Mac Lane, S., 'Mathematics at Göttingen under the Nazis', *Notices of the American Mathematical Society*, vol. 42, no. 10 (1995), pp. 1134 ~ 1138

Neuenschwander, E., 'A brief report on a number of recently discovered sets of notes on Riemann's lectures and on the transmission of the Riemann *Nachlass*', *Historia Mathematica*, vol. 15, no. 2 (1988), pp. 101 ~ 113

Pomerance, C., 'A tale of two sieves', *Notices of the American Mathematical Society*, vol. 43, no. 12 (1996), pp. 1473 ~ 1485 [一篇关于分解整数的文章]

Reid, C., *Hilbert* (New York, NY: Springer, 1970)

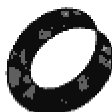
Reid, C., *Julia, A Life in Mathematics* (Washington, DC: Mathematical Association of America, 1996) [包括了 Lisl Gaal、马丁·戴维斯和尤里·马迪亚塞维奇的贡献]

Reid, C., 'Being Julia Robinson's sister', *Notices of the American Mathematical Society*, vol. 43, no. 12 (1996), pp. 1486 ~ 1492

Reid, L. W., *The Elements of the Theory of Algebraic Numbers*, with an Introduction by David Hilbert (New York, NY: Macmillan, 1910)

Ribenboim, P., *The New Book of Prime Number Records* (New York, NY: Springer, 1996)

Sacks, O., *The Man Who Mistook His Wife for a Hat* (New York, NY: Simon & Schuster, 1985)



Sagan, C., *Contact* (New York: Simon & Schuster, 1985)

Schappacher, N., 'Edmund Landau' s Göttingen: from the life and death of a great mathematical center', *The Mathematical Intelligencer*, vol. 13, no. 4 (1991), pp. 12 ~ 18

Schechter, B., *My Brain Is Open. The Mathematical Journeys of Paul Erdös* (New York, NY: Simon & Schuster, 1998)

Schneier, B., *Applied Cryptography*, second edition, (New York, NY: John Wiley, 1996)

Segal, S. L., 'Helmut Hasse in 1934', *Historia Mathematica*, vol. 7, no. 1 (1980), pp. 46 ~ 56

Selberg, A., 'Reflections around the Ramanujan centenary', in *Ramanujan: Essays and Surveys*, History of Mathematics, vol. 22, edited by B. C. Berndt and R. A. Rankin (Providence, RI: American Mathematical Society, 2001), pp. 203 ~ 213

Shimura, G., 'André Weil as I knew him', *Notices of the American Mathematical Society*, vol. 46, no. 4 (1999), pp. 428 ~ 433

Singh, S., *The Code Book* (London: Fourth Estate, 1999)

Struik, D. J., A *Concise History of Mathematics*, (New York, NY: Dover Publication, 1948)

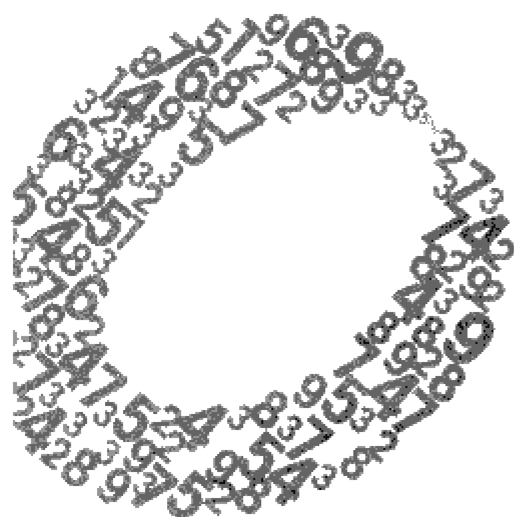
Weil, A., 'Two lectures on number theory, past and present', *L' Enseignement Mathématique*, vol. 20, no. 2 (1974), pp. 87 ~ 110

Weil, A., *Number Theory: An Approach Through History from Hammurapi to Legendre* (Boston, MA: Birkhäuser, 1984)

Weil, A., *The Apprenticeship of a Mathematician*, translated from the 1991 French original by Jennifer Gage (Basel: Birkhäuser, 1992)

Wilson, R., *Four Colours Suffice: How the Map Problem Was Solved* (London: Allen Lan, 2002)

Zagier, D., 'The first 50, 000, 000 prime numbers', *Mathematical Intelligencer*, vol. 0 (1997), pp. 7 ~ 19 [对那些创办该杂志的数学家而言，将这第一份杂志命名为第0卷是很有意义的]



网　站

在上面的阅读材料中，凡是来自 *Notices of the American Mathematical Society* 和 *Bulletin of the American Mathematical Society* 这两本杂志的材料都可以在 http://www.ams.org/notices/和http://www.ams.org/bull/找到在线版本

http://www.musicoftheprimes.com

这是我的网站，其中包括了一些本书的补充材料

http://www.claymath.org

在这里你可以找到所有的7个克莱千禧年问题的描述，以及科纳、怀尔斯和克莱本人的视频资料

http://www.msri.org

伯克利数学科学研究院的网站，其中有大量的视频，也包括一些面向一般观众的视频。

http://www.rsasecurity.com/rsalabs/faq/

http://www.rsasecurity.com/rsalabs/challenges/

在这里你可以找到 RSA 的密码挑战

http://www.mersenne.org/prime.htm



访问这个网站可以加入极大因特网梅森素数搜索计划

http://www.eff.org

有关电子前线基金会为发现大素数者颁发奖金的信息

http://www.maths.ex.ac.uk/~mwatkins/

一个有趣的网站，其中引用的材料都与素数和黎曼假设有关

http://www.certicom.com/research/ecc_chal_contents.html

有关椭圆曲线密码理论的介绍，以及 Certicom 的密码挑战

http://www-groups.dcs.st-andrews.ac.uk/history

"The MacTutor History of Mathematical archive"——由圣安德鲁斯大学开办的数学传记网站

http://www.phys.unsw.edu.au/music/

一个有趣的网站，其中有关于不同乐器的音色与厄斯特·克拉德尼铁盘的关系

http://www.utm.edu/research/primes/

一个很好的关于素数的网站

http://www.naturalsciences.be/expo/ishango/en/index.html

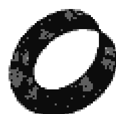
在此你可以看到伊山沟甲骨

http://www.turing.org.uk/

阿兰·图灵传记作者安德鲁·霍奇斯开设的网站

http://www.salon.com/people/feature/1990/10/09/dyson

Kristi Coale 所写的一篇文章"弗里曼·戴森：物理学的青蛙王子"



索 引

注：索引中所标页码代表原书页码（斜体页码代表插图中的标题）

